



ZXR10 8900 Series

10 Gigabit Routing Switch

User Manual (IPv4 Routing Volume)

Version 2.8.02.C

ZTE CORPORATION
ZTE Plaza, Keji Road South,
Hi-Tech Industrial Park,
Nanshan District, Shenzhen,
P. R. China
518057
Tel: (86) 755 26771900
Fax: (86) 755 26770801
URL: <http://ensupport.zte.com.cn>
E-mail: support@zte.com.cn

LEGAL INFORMATION

Copyright © 2006 ZTE CORPORATION.

The contents of this document are protected by copyright laws and international treaties. Any reproduction or distribution of this document or any portion of this document, in any form by any means, without the prior written consent of ZTE CORPORATION is prohibited. Additionally, the contents of this document are protected by contractual confidentiality obligations.

All company, brand and product names are trade or service marks, or registered trade or service marks, of ZTE CORPORATION or of their respective owners.

This document is provided "as is", and all express, implied, or statutory warranties, representations or conditions are disclaimed, including without limitation any implied warranty of merchantability, fitness for a particular purpose, title or non-infringement. ZTE CORPORATION and its licensors shall not be liable for damages resulting from the use of or reliance on the information contained herein.

ZTE CORPORATION or its licensors may have current or pending intellectual property rights or applications covering the subject matter of this document. Except as expressly provided in any written license between ZTE CORPORATION and its licensee, the user of this document shall not acquire any license to the subject matter herein.

ZTE CORPORATION reserves the right to upgrade or make technical change to this product without further notice.

Users may visit ZTE technical support website <http://ensupport.zte.com.cn> to inquire related information.

The ultimate right to interpret this product resides in ZTE CORPORATION.

Revision History

Revision No.	Revision Date	Revision Reason
R1.0	July 31, 2009	First Release

Serial Number: sjzl20093839

Contents

About This Manual.....	i
Safety Instructions.....	1
Safety Introduction.....	1
Safety Description	1
Static Route Configuration	3
Static Route Overview	3
Configuring Static Route	3
Static Route Configuration Examples	4
Static Route Basic Configuration Example	4
Static Route Aggregation Configuration Example	5
Default Route Configuration Example	6
Static Route Maintenance and Diagnosis	7
RIP Configuration.....	9
RIP Overview	9
Metric and Administrative Distance	9
RIP Timers.....	10
Route Update	10
Configuring RIP	10
Enabling RIP	10
Adjusting RIP Timer	11
Configuring RIP Neighbor.....	11
Configuring RIP Authentication	11
Configuring Split Horizon and Poison Reverse	12
Configuring Route Redistribution	12
Configuring RIP Interface Mode	13
Configuring RIP Version	13
RIP Configuration Example.....	13
RIP Maintenance and Diagnosis	14
OSPF Configuration	17
OSPF Overview	17
OSPF Algorithm	18

OSPF Network Types	18
Hello Packet and Timers	19
OSPF Neighbor	19
Adjacency and Designated Router	19
Router Priority and DR Election	20
OSPF Area	20
LSA Types and Diffusion	21
Stub Area and Totally Stubby Area	22
Not-So-Stubby Area	22
OSPF Authentication	23
Configuring OSPF	23
Enabling OSPF	23
Configuring OSPF Interface Timers	23
Configuring OSPF Interface Cost	24
Configuring OSPF Interface Priority	24
Configuring OSPF Neighbor	25
Configuring OSPF Area	25
Configuring Inter-Area Route Aggregation	25
Configuring Default Route Advertisement	26
Configuring Virtual Link	26
Configuring Route Redistribution	27
Configuring OSPF Authentication	27
Configuring Routes to Support Opaque LSA	28
Modifying OSPF Administrative Distance	28
OSPF Configuration Examples	29
Basic OSPF Configuration Example	29
Multi-Area OSPF Configuration Example	30
OSPF Virtual Link Configuration Example	31
OSPF Authentication Configuration Example	33
OSPF Maintenance and Diagnosis	34
IS-IS Configuration	35
IS-IS Overview	35
IS-IS Area	36
IS-IS Network Types	36
DIS and Router Priority	37
Configuring IS-IS	37
Enabling IS-IS	37
Configuring IS-IS Global Parameters	38
Configuring IS-IS Interface Parameters	39
Configuring IS-IS Authentication	40

IS-IS Configuration Examples.....	40
Single-Area IS-IS Configuration Example	40
Multi-Area IS-IS Configuration Example.....	41
IS-IS Maintenance and Diagnosis.....	44
BGP Configuration	45
BGP Overview	45
Configuring BGP	46
Enabling BGP	46
Configuring BGP Route Advertisement	47
Configuring BGP Route Aggregation	49
Configuring EBGp Multi-Hop	50
Filtering Routes through Route Map.....	51
Filtering Routes through NLRI.....	51
Filtering Routes through AS_PATH Attribute.....	52
Configuring LOCAL_PREF Attribute	53
Configuring MED Attribute	55
Configuring Community String Attribute	56
Configuring BGP Synchronization	57
Configuring BGP Route Reflector	59
Configuring BGP Confederation.....	60
Configuring BGP Route Dampening	62
BGP Configuration Example.....	62
BGP Maintenance and Diagnosis	64
Load Sharing Configuration	65
Load Sharing Overview.....	65
Configuring Load Sharing.....	66
Load Sharing Configuration Examples.....	66
Load Sharing through Static Route	66
Load Sharing through OSPF	68
Load Sharing Maintenance and Diagnosis.....	68
Multicast Route Configuration	71
IP Multicast Overview	71
IP Multicast Address.....	71
IGMP	72
Multicast Tree	72
PIM-SM	73
MSDP.....	74
Enabling IP Multicast.....	75
Enabling IP Multicast Load Sharing.....	75
Configuring IGMP	76

Configuring IGMP Version	76
Configuring IGMP Group on Interface	76
Configuring IGMP Timers	77
Configuring Static IP Multicast.....	78
Configuring PIM-SM	79
Enabling PIM-SM	79
Configuring Static RP	80
Configuring Candidate BSR	80
Configuring Candidate RP	81
Applying Static RP for the same RP Priorities	81
Switching over to Source Shortest Path Tree	82
Filtering Received Register Messages.....	82
Filtering Candidate RP	82
Configuring PIM Domain Border	83
Configuring DR Priority	83
Ignoring DR Election	84
Configuring SM/DM Hybrid Mode.....	84
Configuring Hello Message Interval	84
Limiting PIM-SM Neighbors	85
Configuring MSDP	85
Enabling MSDP	85
Configuring Default MSDP Peer.....	86
Configuring Originating RP	86
Configuring MSDP Peer as Mesh Group Member	86
Limiting the Number of SA Messages.....	87
Shutting Down Peers Configured MSDP.....	87
Clearing TCP Connection.....	87
Clearing Entries in MSDP SA Cache	88
Clearing Statistics Counter for MSDP Peers.....	88
IP Multicast Configuration Example	88
IP Multicast Maintenance and Diagnosis	90
Policy Routing Backup Configuration	95
Overview.....	95
Configuring Policy Routing Backup	95
Policy Routing Backup Maintenance and Diagnosis.....	96
IP/LDP FRR Configuration.....	99
IP/LDP FRR Overview	99
Configuring IP/LDP FRR	101
Configuring OSPF FRR	101
Configuring IS-IS FRR	102

Configuring BGP FRR.....	102
Configuring LDP FRR	103
IP/LDP FRR Configuration Example.....	103
OSPF FRR Configuration Example.....	103
IS-IS FRR Configuration Example.....	104
BGP FRR Configuration Example	104
LDP FRR Configuration Example.....	105
IP/LDP FRR Maintenance and Diagnosis	106
BFD Configuration	107
BFD Overview	107
Configuring BFD	108
BFD Configuration Example.....	109
BFD Maintenance and Diagnosis	110
Figures	111
Tables	113
List of Glossary.....	115

About This Manual

Purpose This manual provides procedures and guidelines that support the operation of ZXR10 8900 Series (V2.8.02.C) 10 Gigabit Routing Switch.

Intended Audience This manual is intended for engineers and technicians who perform operation activities on ZXR10 8900 Series (V2.8.02.C) 10 Gigabit Routing Switch.

What Is in This Manual This manual contains the following chapters:

TABLE 1 CHAPTER SUMMARY

Chapter	Summary
Chapter 1 Safety Instructions	This chapter describes the safety instructions and signs
Chapter 2 Static Route Configuration	This chapter describes static route and its configuration, including special summary static route
Chapter 3 RIP Configuration	This chapter describes Routing Information Protocol (RIP) configuration
Chapter 4 OSPF Configuration	This chapter describes Open Shortest Path First (OSPF) protocol and related configuration
Chapter 5 IS-IS Configuration	This chapter describes IS-IS protocol and related configuration
Chapter 6 BGP Configuration	This chapter describes Border Gateway Protocol (BGP) and related configuration
Chapter 7 Load Balance Configuration	This chapter describes Load Balance on ZXR10 8912/8908/8905/8902
Chapter 8 IP Multicast Configuration	This chapter describes basic principle and configuration of IP multicast
Chapter 9 IP/LDP FRR Configuration	This chapter describes IP/LDP FRR on ZXR10 8912/8908/8905/8902
Chapter 10 BFD Configuration	This chapter describes BFD on ZXR10 8912/8908/8905/8902

Related Documentation

The following documentation is related to this manual:

- ZXR10 8900 Series (V2.8.02.C) 10 Gigabit Routing Switch Hardware Installation Manual
- ZXR10 8900 Series (V2.8.02.C) 10 Gigabit Routing Switch Hardware Manual
- ZXR10 8900 Series (V2.8.02.C) 10 Gigabit Routing Switch User Manual (Basic Configuration Volume)

- ZXR10 8900 Series (V2.8.02.C) 10 Gigabit Routing Switch User Manual (Ethernet Switching Volume)
- ZXR10 8900 Series (V2.8.02.C) 10 Gigabit Routing Switch User Manual (IPv4 Routing Volume)
- ZXR10 8900 Series (V2.8.02.C) 10 Gigabit Routing Switch User Manual (MPLS Volume)
- ZXR10 8900 Series (V2.8.02.C) 10 Gigabit Routing Switch User Manual (IPv6 Volume)

Chapter 1

Safety Instructions

Table of Contents

Safety Introduction	1
Safety Description	1

Safety Introduction

In order to operate the equipment in a proper way, follow these instructions:

- Only qualified professionals are allowed to perform installation, operation and maintenance due to the high temperature and high voltage of the equipment.
- Observe the local safety codes and relevant operation procedures during equipment installation, operation and maintenance to prevent personal injury or equipment damage. Safety precautions introduced in this manual are supplementary to the local safety codes.
- ZTE bears no responsibility in case of universal safety operation requirements violation and safety standards violation in designing, manufacturing and equipment usage.

Safety Description

Contents deserving special attention during configuration of ZXR10 8900 series switch are explained in the following table.

Convention	Meaning
Note	Provides additional information
Important	Provides great significance or consequence
Result	Provides consequence of actions
Example	Provides instance illustration

This page is intentionally blank.

Chapter 2

Static Route Configuration

Table of Contents

Static Route Overview	3
Configuring Static Route	3
Static Route Configuration Examples	4
Static Route Maintenance and Diagnosis	7

Static Route Overview

Static Route is that the network administrator specifies routing information to routing table by configuration command, unlike dynamic route creating routing table according to routing algorithm. When configuring dynamic route, sometimes users need to transmit routing information of the whole Internet to a router, which exceeds the load of the router, in such situation, static route can be employed to solve the problem. Application of static route, which requires relatively fewer configurations, can avoid the usage of dynamic route. However, the configuration of static route will become complicated when in the environment with multiple routers and multiple paths.

Configuring Static Route

To configure static route, use the following command.

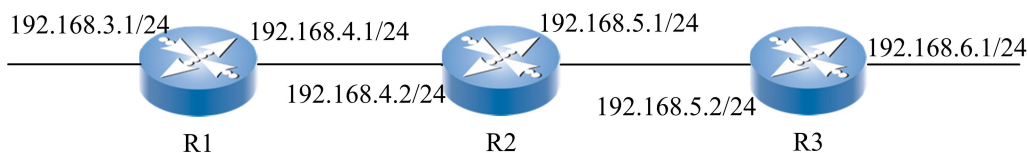
Command	Function
ZXR10 (config) # ip route {{<prefix of destination IP address><network mask>{<next hop address> <interface>}>}<distance metric>}[global][tag <tag value>]} vrf }	This configures static route

Static Route Configuration Examples

Static Route Basic Configuration Example

A simple network with three routers connected is shown in [Figure 1](#).

FIGURE 1 STATIC ROUTE CONFIGURATION



When R1 needs to access network in R3, the static route configuration is shown below.

```

ZXR10_R1(config)#ip route 192.168.5.0 255.255.255.0 192.168.4.2
ZXR10_R1(config)#ip route 192.168.6.0 255.255.255.0 192.168.4.2
  
```

It is seen from the above configuration information that static route is configured in global configuration mode. Only one static route can be configured once. What next to the **ip route** are remote network, subnet mask and next-hop IP address reaching remote network. When R1 wants to transmit message to network 192.168.5.0/24, it must deliver the message to R2 with the IP address of 192.168.4.2; R1 and R2 are connected directly.

Another way to configure static route is shown below.

```

ZXR10_R1(config)#ip route 192.168.5.0 255.255.255.0 vlan2
ZXR10_R1(config)#ip route 192.168.6.0 255.255.255.0 vlan2
  
```

This configuration is similar to the method mentioned above. The only difference is that in the above method, next-hop IP address is applied, while in this method, local interface is applied. It transmits all messages towards network 192.168.5.0/24 and 192.168.6.0/24 from VLAN2 instead of routing to next-hop logical address.

When multiple paths to the same destination are available, configure the router with multiple static routes with different administrative distance values. Routing table only shows the routing information with the minimum distance value. When the router is notified that there are multiple competitive sources to a network, the route with the minimum administrative distance value has a higher priority. Parameter *distance-metric* in **ip route** command can be used to change the administrative distance value of a static route. Assume that there are two different routes from R1 to 192.168.6.0/24 network segment, and the configuration is shown below.

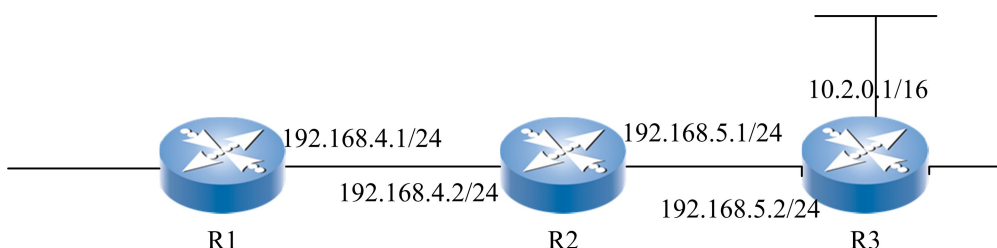
```
ZXR10_R1(config)#ip route 192.168.6.0 255.255.255.0 192.168.4.2
ZXR10_R1(config)#ip route 192.168.6.0 255.255.255.0 192.168.3.2
25 tag 10
```

The above two commands configure two different static routes to the same network. The first command does not configure administrative distance value, so default value 1 is applied. The second command configures the administrative distance value to be 25. The administrative distance value of the first route is smaller than that of the second one, so only the information of the first route is available in the routing table. That is to say, the router reaches the destination network 192.168.6.0/24 through next-hop 192.168.4.2. The second route will be available in the routing table only when the first route becomes invalid and disappears from the routing table.

Static Route Aggregation Configuration Example

Aggregated static route is a special static route, which can summarize expressions of two or multiple specific routing tables into one, to reduce entries of routing table on the basis of remaining all old connections.

FIGURE 2 STATIC ROUTE AGGREGATION CONFIGURATION EXAMPLE



As shown in [Figure 2](#), R3 has two networks including 10.1.0.0/16 and 10.2.0.0/16. Usually, the following two static routes should be configured in R1 to reach these networks.

```
ZXR10_R1(config)#ip route 10.1.0.0 255.255.0.0 192.168.4.2
ZXR10_R1(config)#ip route 10.2.0.0 255.255.0.0 192.168.4.2
```

IP connection can be implemented by the above configuration assuming R3 is properly configured. Summary static route can be used to optimize R1 routing table; the following command can substitute two above commands.

```
ZXR10_R1(config)#ip route 10.0.0.0 255.0.0.0 192.168.4.2
```

This command indicates that all messages with the destination of network 10.0.0.0/8 pass 192.168.4.2, that is to say, all messages of subnets (here refer to subnet 10.1.0.0/16 and 10.2.0.0/16) with the destination of 10.0.0.0/8 transmit to 192.168.4.2. Summarize all subnets of main network 10.0.0.0/8 by this means.

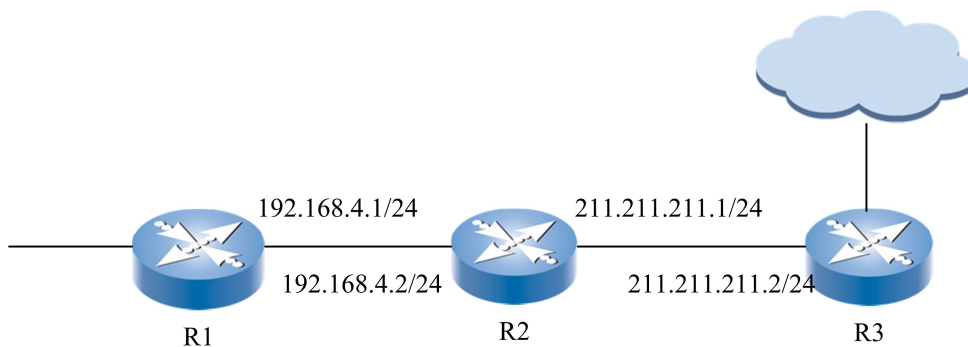
Default Route Configuration Example

Default route is a type of special static route. Default route will be applied when all other routes in the routing table failed, which provides a last destination for the routing table, thus relieving the processing load of the router.

When a router cannot route for a message, the message has to be discarded to an "unknown" destination. To make the router fully connected, one router must be connected to a network. The default route can be applied when the router wants to be fully connected and requires no record of individual route. An individual route can be specified to represent all other routes by default route.

The function and usage of static route are illustrated in the following example.

FIGURE 3 DEFAULT ROUTE CONFIGURATION EXAMPLE



As shown in [Figure 3](#), R2 and router R3 in the Internet network are connected. R2 did not record all network addresses in the Internet, it uses default route to directly transmit unknown messages to R3. The configuration of default route in R2 is shown below.

```
ZXR10_R2(config)#ip route 0.0.0.0 0.0.0.0 211.211.211.2
```

Configuration procedure of default route is identical with that of static route. The difference is that both the network part and subnet mask part are 0.0.0.0. Routing table of R2 is shown below.

```
ZXR10_R2#show ip route
IPv4 Routing Table:

```

Dest	Mask	Gw	Net	Owner
211.211.211.0	255.255.255.0			direct
192.168.4.0	255.255.255.0			direct
0.0.0.0	0.0.0.0	211.211.211.2		static

```
ZXR10_R2#
```

It is seen from the routing table, that the default route with next-hop of 211.211.211.2 is added to the routing table as the last route.

When using default route in routing protocol configuration, it differs when routing protocol varies.

When default route is configured in a router running RIP protocol, RIP will notify the default route 0.0.0.0/0 to its neighbor, even not need to reallocate routes in the RIP domain.

For OSPF protocol, the router running OSPF will not notify default route automatically to its neighbor. **Default-information originate** command must be used to enable OSPF to transmit default route to OSPF domain. When reallocating default routes in the OSPF domain, this kind of notification is usually implemented by ASBR (Autonomous System Border Router).

Static Route Maintenance and Diagnosis

To view global routing table of router and to view whether static route is configured in routing table, use the following command.

Command	Function
ZXR10# show ip route [<i><ip-address></i> [<i><net-mask></i>]] <i><protocol></i>]	This views global routing table of router and views whether static route is configured in routing table

This page is intentionally blank.

RIP Configuration

Table of Contents

RIP Overview	9
Configuring RIP	10
RIP Configuration Example.....	13
RIP Maintenance and Diagnosis	14

RIP Overview

Routing Information Protocol ([RIP](#)) is the first routing protocol identifying the best path dynamically, which is implemented based on vector distance algorithm of local network. RIPv1 is defined in [RFC1058](#) and RIPv2 is defined in RFC1723. ZXR10 8900 series switch supports both RIPv1 and RIPv2, RIPv2 is applied by default. RIPv2 has the following advantages compared to RIPv1:

- Subnet mask is available in route refresh
- Authentication of route refresh
- Multicasting route refresh

In the following instruction, RIP refers to RIPv2 if not specially designated.

Metric and Administrative Distance

RIP uses [UDP](#) packet (Port number 520) to exchange RIP routing information. The routing information in RIP message includes the number of routes passed, that is, hop count, according to which, router determines the route to the destination network. RFC stipulates that the maximum hop count should be less than 16, so RIP is only applicable to small-sized network. Hop count 16 indicates infinite distance, representing unreachable route, which is one way for RIP to identify and prevent the routing loop.

Only hop count is taken as the metric for RIP routing; bandwidth, delay and other variable factors are not considered. RIP always takes paths with the least hop count as the optimized path, which may results that the selected path is not the best one.

Default administrative distance value of RIP is 120. As far as [AD](#) is concerned, the lower is the value; the higher is the routing source

reliability. Comparing with other routing protocol, RIP is not quite reliable.

RIP Timers

Router running RIP transmits update message of routing information at a certain interval (30s by default), which reflects all the routing information of the router. This process is called routing information notification. When a router fails to receive update information from another router in a certain time period (180s by default), it marks the routes provided by the router to be "unavailable". When it is not updated in the succeeding period of time (240s by default), the router clears the route completely from the routing table.

RIP provides the following four types of timers:

- Update timer
- Invalid timer
- Hold-down timer
- Flush Timer

Route Update

RIP protocol employs trigger update to speed up the spread of routing changes in the RIP routing domain. When a RIP router detects that an interface is working or has stopped working, an adjacent node is down or a new subnet or neighbor node joins in, it will transmit a trigger update. The trigger update message only contains changed route.

RIP protocol uses poison reverse to speed up protocol convergence. The poison reverse sets the metrics of the infinite network prefix to be 16 (meaning infinite), after receiving routing update of the metric, the router will discard the route instead of waiting for the aging time.

RIP uses split horizon to prevent routing loop and reduce the size of routing update. Split horizon means that if an interface receives a routing update, it will not transmit this update from itself to others.

Configuring RIP

Enabling RIP

To enable RIP, perform the following steps.

Step	Command	Function
1	ZXR10 (config) # router rip	This starts RIP routing process
2	ZXR10 (config-router) # network <ip-address><wildcard-mask>	This defines interface on which RIP is configured

Adjusting RIP Timer

To adjust RIP timers, perform the following steps.

Step	Command	Function
1	ZXR10 (config) # router rip	This starts RIP routing process
2	ZXR10 (config-router) # timers basic <update><invalid><holddown><flush>	This adjusts basic timers
3	ZXR10 (config-router) # output-delay <packets><delay>	This changes inter-message-group delay of RIP update packet

Configuring RIP Neighbor

To configure RIP neighbor, perform the following steps.

Step	Command	Function
1	ZXR10 (config) # router rip	This starts RIP routing process
2	ZXR10 (config-router) # neighbor <ip-address>	This defines the adjacent router exchanging routing information with this router

Configuring RIP Authentication

In order to strengthen the security of routing process, configure RIP authentication in the router. Set interface password; the network neighborhood must use the same password in the network.

To configure authentication, perform the following steps.

Step	Command	Function
1	ZXR10 (config) # interface vlan <vlan-id>	This enters VLAN Layer 3 interface configuration mode
2	ZXR10 (config-if) # ip rip authentication mode {text md5}	This configures authentication type

Step	Command	Function
3	<code>ZXR10(config-if)#ip rip authentication key <key></code>	This specifies the password value for interface simple text authentication
4	<code>ZXR10(config-if)#ip rip authentication key-chain <key-chain></code>	This specifies the password value for interface MD5 authentication

**Note:**

RIPv2 supports simple text authentication and MD5 authentication. RIPv1 does not support authentication.

Configuring Split Horizon and Poison Reverse

To configure split horizon and poison reverse, perform the following steps.

Step	Command	Function
1	<code>ZXR10(config)#interface vlan <vlan-id></code>	This enters VLAN Layer 3 interface configuration mode
2	<code>ZXR10(config-if)#ip split-horizon</code>	This enables split horizon mechanism
3	<code>ZXR10(config-if)#ip poison-reverse</code>	This enables poison reverse mechanism

Configuring Route Redistribution

To configure route redistribution, perform the following steps.

Step	Command	Function
1	<code>ZXR10(config)#router rip</code>	This starts RIP routing process
2	<code>ZXR10(config-router)#redistribute <protocol>[metric <metric-value>][route-map <name>]</code>	This redistributes route of another route protocol to RIP route domain
3	<code>ZXR10(config-router)#default-metric <metric-value></code>	This sets default metric of redistributed route

Configuring RIP Interface Mode

To configure RIP interface mode, perform the following steps.

Step	Command	Function
1	ZXR10 (config) # interface vlan <vlan-id>	This enters VLAN Layer 3 interface configuration mode
2	ZXR10 (config-if) # ip rip interface { active passive }	This configures the working mode of an interface



Note:

When the interface is in active mode, the interface can send and receive RIP messages. When the interface is in passive mode, the interface can only receive RIP messages.

Configuring RIP Version

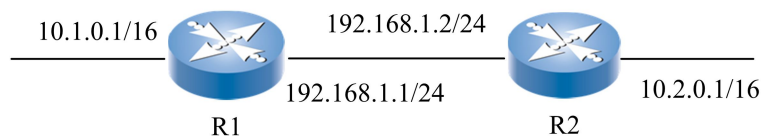
To configure RIP version, perform the following steps.

Step	Command	Function
1	ZXR10 (config) # router rip	This starts RIP routing process
2	ZXR10 (config-router) # version { 1 2 }	This configures RIP version. By default, it is RIPv2
3	ZXR10 (config-router) # exit	This exits RIP route configuration mode
4	ZXR10 (config) # interface vlan <vlan-id>	This enters VLAN Layer 3 interface configuration mode
5	ZXR10 (config-if) # ip rip receive version { 1 2 }[1 2]	This configures RIP version that is received on interface
6	ZXR10 (config-if) # ip rip send version { 1 2 { broadcast multicast }}	This configures RIP version that is transmitted at interface

RIP Configuration Example

As shown in [Figure 4](#), R1 and R2 run RIP.

FIGURE 4 RIP CONFIGURATION EXAMPLE



Configuration on R1:

```

ZXR10_R1(config)#router rip
ZXR10_R1(config-router)#network 10.1.0.0 0.0.255.255
ZXR10_R1(config-router)#network 192.168.1.0 0.0.0.255

```

Configuration on R2:

```

ZXR10_R2(config)#router rip
ZXR10_R2(config-router)#network 10.2.0.0 0.0.255.255
ZXR10_R2(config-router)#network 192.168.1.0 0.0.0.255

```

RIP Maintenance and Diagnosis

To configure RIP maintenance and diagnosis, perform the following steps.

Step	Command	Function
1	<code>ZXR10#show ip rip [vrf <vrf-name>]</code>	This views protocol information
2	<code>ZXR10#show ip rip interface [vrf <vrf-name>]<interface-name></code>	This views current configuration and status of RIP interface
3	<code>ZXR10#show ip rip neighbors</code>	This views information of all configured neighbors
4	<code>ZXR10#show ip rip database [vrf <vrf-name>][network <ip-address>[mask <net-mask>]]</code>	This views routing entries generated by RIP protocol
5	<code>ZXR10#show ip rip networks [vrf <vrf-name>]</code>	This views all RIP interface information
6	<code>ZXR10#debug ip rip</code>	This tracks RIP basic process of transmitting and receiving packet
7	<code>ZXR10#debug ip rip database</code>	This tracks the change process of RIP routing table

Example This example shows RIP debugging information.

```

ZXR10#debug ip rip
RIP protocol debugging is on
ZXR10#
11:01:28: RIP: building update entries

```

```
130.1.0.0/16 via 0.0.0.0, metric 1, tag 0
130.1.1.0/24 via 0.0.0.0, metric 1, tag 0
177.0.0.0/9 via 0.0.0.0, metric 1, tag 0
193.1.168.0/24 via 0.0.0.0, metric 1, tag 0
197.1.0.0/16 via 0.0.0.0, metric 1, tag 0
199.2.0.0/16 via 0.0.0.0, metric 1, tag 0
202.119.8.0/24 via 0.0.0.0, metric 1, tag 0
11:01:28: RIP: sending v2 periodic update to 224.0.0.9
via vlan10 (193.1.1.111)
130.1.0.0/16 via 0.0.0.0, metric 1, tag 0
130.1.1.0/24 via 0.0.0.0, metric 1, tag 0
177.0.0.0/9 via 0.0.0.0, metric 1, tag 0
193.1.1.0/24 via 0.0.0.0, metric 1, tag 0
11:01:28: RIP: sending v2 periodic update to 193.1.168.95
via vlan20 (193.1.168.111)
11:01:28: RIP: sending v2 periodic update to 193.1.168.86
via vlan20 (193.1.168.111)
11:01:28: RIP: sending v2 periodic update to 193.1.168.77
via vlan20 (193.1.168.111)
11:01:28: RIP: sending v2 periodic update to 193.1.168.68
via vlan20 (193.1.168.111)
```

This page is intentionally blank.

OSPF Configuration

Table of Contents

OSPF Overview	17
Configuring OSPF	23
OSPF Configuration Examples.....	29
OSPF Maintenance and Diagnosis.....	34

OSPF Overview

Open Shortest Path First ([OSPF](#)) is one of the most popular and widely-used protocols presently. OSPF is a link-state protocol, which overcomes the disadvantages of RIP and other distance-vector protocols. OSPF is an open standard, which makes devices of different vendors interconnect with each other through protocol.

OSPF version 1 is defined in RFC1131. Currently used OSPF version 2 is defined in RFC2328. ZXR10 8900 series switch completely supports OSPF version 2.

OSPF has the following characteristics:

- Fast convergence, which ensures database synchronization by fast diffusing link state update, and calculates routing table synchronously.
- Loop-free, which ensures that no loop generated by SPF algorithm.
- Aggregation, reduce size of routing table.
- Totally classless, which supports Variable Length Subnet Mask ([VLSM](#)) and Classless Inter-Domain Routing ([CIDR](#)).
- Reducing the required network bandwidth; for trigger update mechanism is adopted, only when the network changes, the update information is transmitted.
- Supporting interface packet authentication, ensuring security of routing calculation.
- Transmitting update through multicast mode, which reduces interference against unrelated network devices while broadcasting.

OSPF Algorithm

As OSPF is a link state protocol. OSPF router generates the routing table by setting up a link state database which contains the information of all networks and routers. Routers use this information to establish routing tables. To ensure reliability, all routers must have the completely same link state database.

Link state database is built based on Link State Advertisements (LSAs) which are generated by all routers and spread over the whole OSPF network. There are many types of LSAs, a complete LSA set shows an accurate distribution diagram over the whole network.

OSPF uses cost as the metric. Cost is distributed to each port of a router. A port calculates the cost based on 100M benchmark by default. The path cost to a particular destination is the total cost of all links between the router and the destination.

To generate a routing table based on LSA database, a router run the Dijkstra SPF algorithm to construct a cost routing tree with itself as the root of the routing tree. The Dijkstra algorithm enables a router to calculate the lowest-cost path between itself and any node on the network. Router saves the routes of the paths in the routing table.

Different from RIP, OSPF does not simply broadcast all its routing information regularly. An OSPF router sends call messages to its neighbors to let them know it is still alive. When a router does not receive any message from a neighbor within a period of time then the neighbor might not be alive.

OSPF routing is incrementally updated. Router sends the update information only when topology changes. When the age of an LSA reaches 1800 seconds, a new version of the LSA is resent.

OSPF Network Types

The type of the network connecting to a port is used to determine the default OSPF behavior on that port. The network type affects the adjacency relationship and how the router designates a timer to the port.

There are five network types in OSPF, and they are as follows:

- Broadcast
- Non-broadcast Multi-access (NBMA)
- Point-to-Point
- Point-to-Multipoint
- Virtual Links

Hello Packet and Timers

OSPF router exchanges Hello packet at a certain interval, whose function is to keep alive among neighbors. Hello packet can detect OSPF neighbor, create association and adjacency among neighbors, and select designated router. In broadcast and point-to-point network types, Hello packets are multicast packets; in NBMA network, point-to-multipoint and virtual links, Hello packets are unicast packets.

OSPF uses three kinds of hello-packet-related timers:

- Calling Interval

Calling interval is a property of interface, which defines the interval of sending hello packets by the router from each interface. The default calling interval is determined by the network type. In the broadcast and point-to-point network, the default calling interval is 10 seconds; while in NBMA and point-to-multipoint network, the default calling interval is 30 seconds. The adjacent routers must accept the length of calling interval so as to become neighbors.

- Router dead-interval

The router dead-interval refers to the waiting time from the router receiving the last hello packet from neighbor to the router detecting that the neighbor is offline. The default router dead-interval is four times of calling interval, which is applicable to all network types.

- Poll Interval

Poll interval is only applied in NBMA network.

OSPF Neighbor

OSPF neighbor is a group of routers in the same network; these routers stipulated some configuration parameters. The routers must be neighbors then they can become adjacent with neighbor.

Analyze hello packets mutually when the routers form neighbor relationship to make sure that the required parameters are stipulated. The parameters cover: Area ID, area flag, authentication information, calling interval, and router dead interval.

Adjacency and Designated Router

When two routers become adjacent, they can exchange routing information. The network type connecting routers determines whether two routers become adjacent.

Point-to-point network and virtual link have only two routers, so the routers become adjacent automatically. Point-to-multipoint network can be considered to be the aggregation of point-to-point network, every pair of routers become adjacent.

Neighbors do not necessarily have the adjacency relationship on broadcast and NBMA networks. If all n routers on a network have set up the adjacency relationship, each router has $(n-1)$ adjacency relationships and there are $n(n-1)/2$ adjacency relationships on the network. Tracking so many adjacency relationships on a large multi-access network will impose a heavy burden on each router. Routing information between each pair of neighbor routers will waste a great deal of network bandwidth.

Therefore, OSPF defines a Designated Router (DR) and a Backup Designated Router (BDR). DR has the following duties:

- To represent the multi-access network and its attached routers to the rest of the internet work.
- To manage the flooding process on the multi-access network.

DR and BDR must establish an adjacency relationship with each OSPF router on the network. Each OSPF router only establishes adjacency relationships with DR and BDR. If the DR stops working then BDR will take its place and becomes DR.

Router Priority and DR Election

Each router has a priority, which will affect the router's capability of becoming DR or BDR in the connected network. The router priority is indicated by octet unsigned integer, with the range of 0~255, 1 by default.

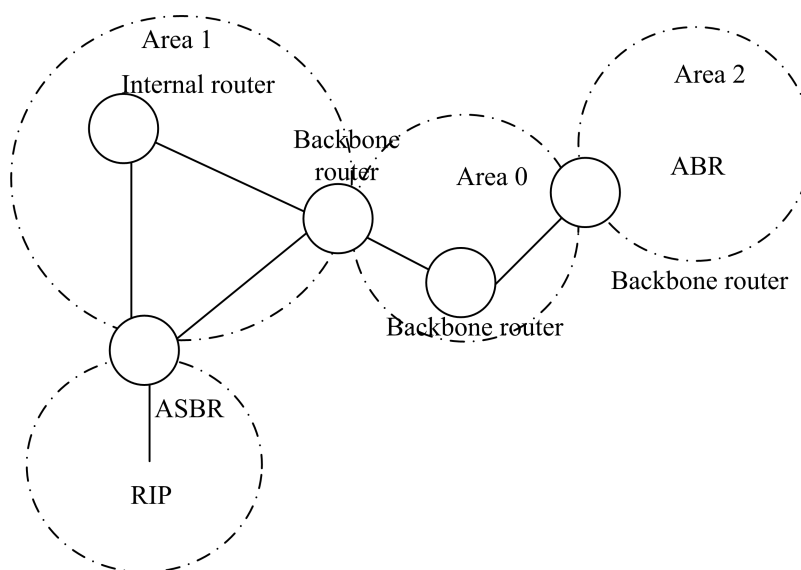
In DR election, the router with the highest priority will become the DR. When the priorities are the same, the router with the highest election IP address is the DR. The router with the priority of 0 cannot become DR or BDR.

OSPF Area

OSPF divides the network into several minor parts to reduce the information size that each router stores and maintains. Each router must have the integrated information of the area it resides in. Areas can share their information. Routing information can be filtered, which can reduce the size of routing information saved in the router.

One area is identified with 32-bit unsigned number. Area 0 is reserved to identify backbone network, all other areas must be connected with area 0. An OSPF network must have a backbone area. Routers can be one or multiple of the following types according to its tasks in the area, as shown in [Figure 5](#).

FIGURE 5 OSPF ROUTER TYPES



- Internal router: A router that has all of its interfaces within the same area.
- Backbone router: A router that has at least one interface in area 0.
- Area Border Router (ABR): A router that has at least one interface in area 0 and at least one interface in other area.
- Autonomous System Border Router (ASBR): The router connects an AS running OSPF to another AS running other protocols (such as RIP or IGRP).

LSA Types and Diffusion

LSA is the way of exchanging information for link state database between OSPF routers; the router uses LSA to construct a precise and complete network view, and generates routes used in the routing table. ZXR10 8900 series switch supports 6 types of LSA. They are respectively:

- Type 1: Router LSA
- Type 2: Network LSA
- Type 3: Network summary LSA
- Type 4: ASBR summary LSA
- Type 5: AS external LSA
- Type 7: NSSA external LSA

The OSPF operation is determined by all the routers in an area sharing a public link state database, therefore, all LSAs need to be diffused by this area, at the same time, processing must be reliable. Every router receiving LSA of specific area will diffuse it to other interfaces belonging to this area. LSAs do not have their own message formats. LSAs are contained in the Link State

Update (LSU) messages. Several LSAs can be contained in one LSU. When the router receives a LSU, it separates the messages from LSA and inputs them into its own database rather than simply transmit the message. Meanwhile, the router constructs its own LSU and transmits the updated LSU to its adjacent neighbors.

The OSPF uses Link State Acknowledgements (LSAck) to confirm whether each LSA is received by the neighbor successfully. An LSAck has identified LSA header, which provides efficient information to identify an LSA uniquely. When a router sends an LSA to an interface, the LSA will be recorded in the retransmission queue of the interface. The router will wait for the maximum interval to receive the LSAck of the LSA. If it fails to receive LSAck in the stipulated time, the router will retransmit the LSA. The router can adopt unicast or multicast to transmit old LSU, but the retransmitted LSU is unicast.

Stub Area and Totally Stubby Area

When ASBR is not available in a non-backbone, the router has only one path to AS external network, namely, by ABR. Therefore, routers in these areas will transmit the LSA which are transmitted towards AS external unknown hosts to ABR. As a result, type 5 LSA is not required to be diffused to the area, and in this area, there is no LSA of type 4. This kind of area type is called Stub Area.

In a stub area, all routers must be configured to be stub routers. Hello packet contains a "stub area" flag bit, which must be consistent in the neighbors.

The ABR in the stub area can filter type 5 LSA to prevent them from releasing in the stub area. At the same time, ABR will generate a type 3 LSA, notifying a default route reached AS external destination address.

If the ABR also filters type 3 LSA, and notifies a default route reached area external destination address. This kind of area is called Totally Stubby Area.

Not-So-Stubby Area

Routers in stub area do not permit type 5 LSA, so ASBR is not a part of stub area. However, users may expect a stub area with ASBR, in which, the router receives AS external routes from the ASBR in this area, but external routing information from other areas will be blocked.

OSPF defines Not-So-Stubby Area (NSSA). In an NSSA, ASBR generates type 7 LSA instead of type 5 LSA. The ABR cannot transmit type 7 LSA to other OSPF area. On the one hand, it blocks the external routers from reaching the NSSA area, on the other hand, it converts type 7 LSA into type 5 LSA.

OSPF Authentication

Authentication can be applied in packet switching between two OSPF neighbors. The neighbors must agree on authentication type, which is contained in all packets. This is shown in [Table 3](#).

TABLE 3 OSPF AUTHENTICATION

Value	Description
0	No authentication
1	Simple text authentication
2	MD5 authentication

When configuring simple password authentication, one interface allows only one password, the password of each interface can be different, but in a specific network, every interface must have identical password. Simple password is transmitted by OSPF packets through clear text.

Configuring OSPF

Enabling OSPF

To enable OSPF, perform the following steps.

Step	Command	Function
1	ZXR10 (config) # router ospf <process-id> [vrf <vrf-name>]	This enables OSPF process
2	ZXR10 (config-router) # network <ip-address> <wildcard-mask> area <area-id>	This defines interface which runs OSPF and the area which the interface belongs to

Configuring OSPF Interface Timers

Many OSPF characteristics can be self-defined to adapt to any network environment. Although in most cases, it is not necessary to modify the default value of the timer, sometimes, adjusting timer can improve the protocol performance.

To configure OSPF interface timers, perform the following steps.

Step	Command	Function
1	ZXR10 (config) # interface vlan <vlan-id>	This enters VLAN Layer 3 interface configuration mode
2	ZXR10 (config-if) # ip ospf hello-interval <seconds>	This configures Hello message transmission interval
3	ZXR10 (config-if) # ip ospf retransmit-interval <seconds>	This configures LSA retransmission interval
4	ZXR10 (config-if) # ip ospf transmit-delay <seconds>	This configures transmission delay of link state update packet
5	ZXR10 (config-if) # ip ospf dead-interval <seconds>	This configures dead time of neighbors

Configuring OSPF Interface Cost

To configure OSPF interface cost, perform the following steps.

Step	Command	Function
1	ZXR10 (config) # interface vlan <vlan-id>	This enters VLAN Layer 3 interface configuration mode
2	ZXR10 (config-if) # ip ospf cost <cost>	This sets interface cost



Note:

When using network devices of multiple vendors, make sure that all OSPF can work together. For example, all routers must use the same method to calculate interface cost.

Configuring OSPF Interface Priority

To configure OSPF interface priority, perform the following steps.

Step	Command	Function
1	ZXR10 (config) # interface vlan <vlan-id>	This enters VLAN Layer 3 interface configuration mode
2	ZXR10 (config-if) # ip ospf priority <priority>	This sets interface priority

Configuring OSPF Neighbor

To configure neighbor, perform the following steps.

Step	Command	Function
1	ZXR10 (config) # router ospf <process-id> [vrf <vrf-name>]	This enables OSPF process
2	ZXR10 (config-router) # neighbor <ip-address> [cost <cost>] [priority <priority>] [poll-interval <seconds>]	This configures neighbor router in the non-broadcast network

Configuring OSPF Area

OSPF uses area to implement hierarchical routing. OSPF area covers stub area, totally stubby area, and not-so-stubby area. The backbone area belongs to conversion area.

To configure OSPF area, use one of the following commands.

Command	Function
ZXR10 (config-router) # area <area-id> stub [default-cost <cost>]	This configures an area to be stub area
ZXR10 (config-router) # area <area-id> stub no-summary [default-cost <cost>]	This configures an area to be totally stubby area
ZXR10 (config-router) # area <area-id> nssa [no-redistribution] [default-information-originate [metric <metric-value>] [metric-type <type>]] [no-summary]	This configures an area to be not-so-stubby area

Configuring Inter-Area Route Aggregation

One of the reasons for OSPF's prevalence is route aggregation. The router aggregation can occur between areas or between autonomous systems. The inter-area route aggregation occurs in ABR, while inter-autonomous-systems route aggregation occurs in ASBR.

Configuring stub area can save route resources in the stub area but it does not help the backbone network. When network address distribution in an area is consecutive, configure ABR to advertise a converged route to replace these consecutive single routes. The route aggregation can save backbone resources. It is implemented by advertising a group of network addresses to be an aggregation address.

To configure inter-area route aggregation, perform the following steps.

Step	Command	Function
1	<code>ZXR10(config)#router ospf <process-id>[vrf <vrf-name>]</code>	This enables OSPF process
2	<code>ZXR10(config-router)#area <area-id> range <ip-address><net-mask>[advertise not-advertise]</code>	This configures the summary address range in the area

Configuring Default Route Advertisement

Configure an ASBR to advertise a default route to the entire OSPF area. A router becomes an ASBR after using redistribution route. By default, ASBR does not advertise default route to the entire OSPF area automatically. Configure router to notify default route by command, then the router becomes ASBR automatically.

To configure default route advertisement, perform the following steps.

Step	Command	Function
1	<code>ZXR10(config)#router ospf <process-id>[vrf <vrf-name>]</code>	This enables OSPF process.
2	<code>ZXR10(config-router)#notify default route [always][metric <metric-value>][metric-type <type>][route-map <name>]</code>	This configures ASBR to advertise default route to OSPF area.

Configuring Virtual Link

All areas in the OSPF network must be connected to backbone area directly. This restricts the area layout, especially when the network is vast. To solve this problem, connect a remote area through other area to backbone area by means of virtual link. The area that the virtual link crossed must have complete routing information. So the area cannot be a stub area.

To configure virtual link, perform the following steps.

Step	Command	Function
1	<code>ZXR10(config)#router ospf <process-id>[vrf <vrf-name>]</code>	This enables OSPF process
2	<code>ZXR10(config-router)#area <area-id> virtual-link <router-id>[hello-interval <seconds>][retransmit-interval <seconds>][transmit-delay <seconds>][dead-interval <seconds>][authentication-key <key>][message-digest-key <keyid> md5 <cryptkey>][delay <time>][authentication [null message-digest]]</code>	This configures virtual link

Configuring Route Redistribution

Different dynamic routing protocols can share routing information through route redistribution. In OSPF, the routing information of other routing protocol is external routing information of autonomous system. It can be diffused to the entire OSPF network through OSPF LSA only when it is redistributed to OSPF protocol.

Each individual route is advertised as an external LSA when routes of other protocols are redistributed to OSPF. Use route aggregation to advertise these routes. This reduces the size of OSPF link state database significantly.

To configure route redistribution, perform the following steps.

Step	Command	Function
1	ZXR10 (config) # router ospf <process-id> [vrf <vrf-name>]	This enables OSPF process
2	ZXR10 (config-router) # redistribute <protocol> [as <as-number>] [peer <peer-address>] [tag <tag-value>] [metric <metric-value>] [metric-type <type>] [route-map <name>]	This redistributes other routing protocols to OSPF autonomous system and make the router to be an ASBR
3	ZXR10 (config-router) # summary-address <ip-address> <net-mask>	This constructs aggregation address for OSPF and summarizes other routing protocol routes that are redistributed to OSPF

Configuring OSPF Authentication

In order to enhance the security of routing process in the network, configure OSPF authentication on router. To set interface password, the network neighborhood must use the same password in the network.

To configure OSPF authentication, perform the following steps.

Step	Command	Function
1	ZXR10 (config) # router ospf <process-id> [vrf <vrf-name>]	This enables OSPF process
2	ZXR10 (config-router) # area <area-id> authentication [message-digest]	This enables authentication in OSPF area
3	ZXR10 (config-router) # exit	This exits OSPF route configuration mode
4	ZXR10 (config) # interface vlan <vlan-id>	This enters VLAN Layer 3 interface configuration mode
5	ZXR10 (config-if) # ip ospf authentication [null message-digest]	This sets authentication type of interface

Step	Command	Function
6	<code>ZXR10(config-if)#ip ospf authentication-key <password></code>	This sets key for the interface with the type of simple text authentication
7	<code>ZXR10(config-if)#ip ospf message-digest-key <key id> md5 <password>[encrypt][delay <time>]</code>	This sets key for the interface with the type of MD5 authentication

Configuring Routes to Support Opaque LSA

In the process of link state database switching, the opaque LSA is contained in database abstract list and transmitted to the adjacent routers that do not support opaque LSA.

When a router floods opaque LSA to adjacent router, it first checks whether the adjacent router supports opaque LSA. The opaque LSA is only transmitted to the adjacent routers that support this function. They are added to the link state retransmission list of the adjacent router. When the link state update report is a multicast packet, the adjacent routers that do not support this function will receive this advertisement passively and then simply discard.

To configure routes to support opaque LSA, perform the following steps.

Step	Command	Function
1	<code>ZXR10(config)#router ospf <process-id>[vrf <vrf-name>]</code>	This enables OSPF process
2	<code>ZXR10(config-router)#capability opaque</code>	This configures routes to support opaque LSA

Modifying OSPF Administrative Distance

Administrative distance represents the reliability of information source. Administrative distance is an integer in the range of 0~255. The higher value is, the lower reliability is. When administrative distance is 255, it means that the routing information source is unreliable.

To modify OSPF administrative distance, perform the following steps.

Step	Command	Function
1	ZXR10 (config) # router ospf <process-id>[vrf <vrf-name>]	This enables OSPF process
2	ZXR10 (config-router) # distance ospf {[internal <distance>][ext1 <distance>][ext2 <distance>]}	This modifies OSPF administrative distance

**Note:**

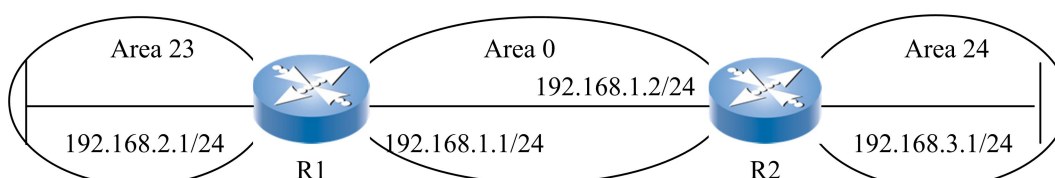
ZXR10 8900 series switch defines three types of administrative distances of OSPF routes: internal route, type 1 external route and type 2 external routes. By default, administrative distances of the three types of routes are 110.

OSPF Configuration Examples

Basic OSPF Configuration Example

As shown in [Figure 6](#), run OSPF in routers R1 and R2 and divide the network into three areas.

FIGURE 6 BASIC OSPF CONFIGURATION EXAMPLE



Configuration on R1:

```

ZXR10_R1(config)#router ospf 1
ZXR10_R1(config-router)#network 192.168.2.0 0.0.0.255 area 23
ZXR10_R1(config-router)#network 192.168.1.0 0.0.0.255 area 0
  
```

Configuration on R2:

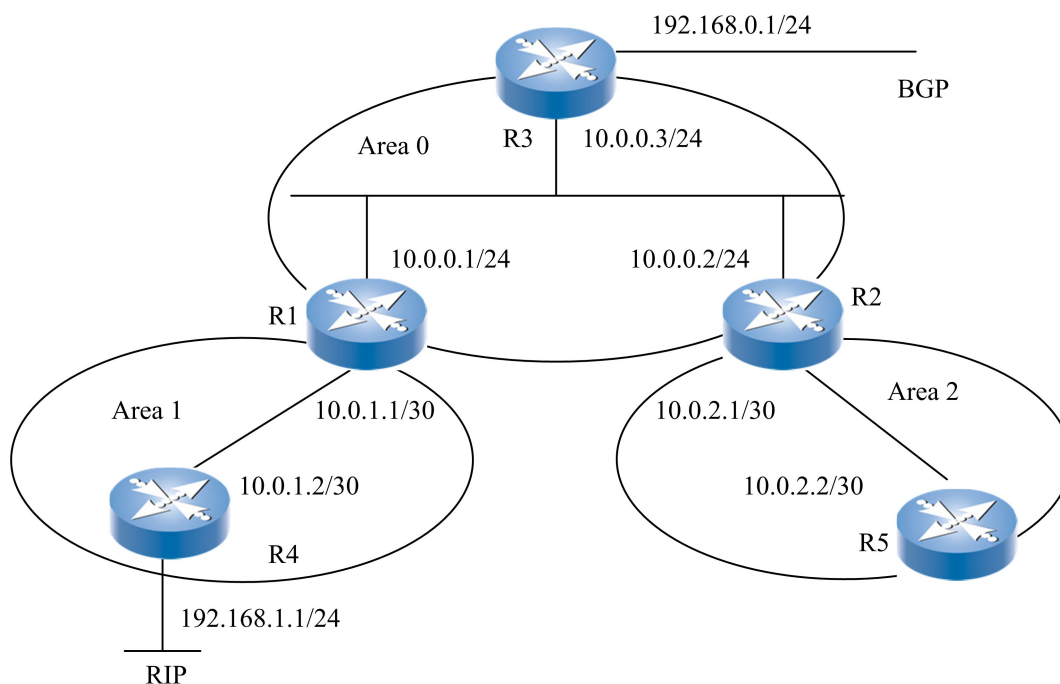
```

ZXR10_R2(config)#router ospf 1
ZXR10_R2(config-router)#network 192.168.3.0 0.0.0.255 area 24
ZXR10_R2(config-router)#network 192.168.1.0 0.0.0.255 area 0
  
```

Multi-Area OSPF Configuration Example

A multi-area OSPF network topology is in [Figure 7](#).

FIGURE 7 MULTI-AREA OSPF CONFIGURATION EXAMPLE



Area 1 is an NSSA area. R1 is an ABR working between NSSA area 1 and backbone area. R1 advertises a default route to this area.

Area 2 is a stub area. R2 is an ABR working between area 2 and backbone area. In the stub area, ABR advertises a default route to stub area automatically.

R3 is a router working in backbone area 0. It connects to other autonomous system by BGP. As the exit router of the entire autonomous system, R3 advertises a default route to the entire OSPF area by manual configuration.

R4 is an ASBR in NSSA area 1. It also runs RIP protocol besides OSPF. RIP protocol is injected into OSPF by route redistribution.

R5 is a router working in stub area 2.

Configuration on R1:

```
ZXR10_R1(config)#interface vlan1
ZXR10_R1(config-if)#ip address 10.0.1.1 255.255.255.252
ZXR10_R1(config-if)#exit
ZXR10_R1(config)#interface vlan2
ZXR10_R1(config-if)#ip address 10.0.0.1 255.255.255.0
ZXR10_R1(config-if)#exit
ZXR10_R1(config)#router ospf 1
ZXR10_R1(config-router)#network 10.0.0.0 0.0.0.255 area 0
ZXR10_R1(config-router)#network 10.0.1.0 0.0.0.3 area 1
ZXR10_R1(config-router)#area 1 nssa default-information-originate
```

Configuration on R2:

```
ZXR10_R2(config)#interface vlan1
ZXR10_R2(config-if)#ip address 10.0.2.1 255.255.255.252
ZXR10_R2(config-if)#exit
ZXR10_R2(config)#interface vlan2
ZXR10_R2(config-if)#ip address 10.0.0.2 255.255.255.0
ZXR10_R2(config-if)#exit
ZXR10_R2(config)#router ospf 1
ZXR10_R2(config-router)#network 10.0.0.0 0.0.0.255 area 0
ZXR10_R2(config-router)#network 10.0.2.0 0.0.0.3 area 2
ZXR10_R2(config-router)#area 2 stub
```

Configuration on R3:

```
ZXR10_R3(config)#interface vlan1
ZXR10_R3(config-if)#ip address 10.0.0.3 255.255.255.0
ZXR10_R3(config-if)#exit
ZXR10_R3(config)#interface vlan2
ZXR10_R3(config-if)#ip address 192.168.0.1 255.255.255.0
ZXR10_R3(config-if)#exit
ZXR10_R3(config)#router ospf 1
ZXR10_R3(config-router)#network 10.0.0.0 0.0.0.255 area 0
ZXR10_R3(config-router)#notify default route always
```

Configuration on R4:

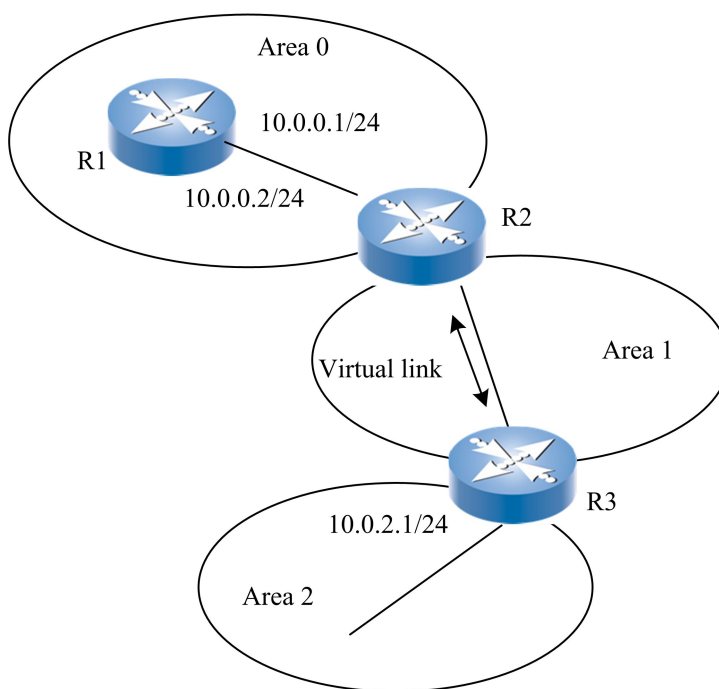
```
ZXR10_R4(config)#interface vlan1
ZXR10_R4(config-if)#ip address 192.168.1.1 255.255.255.0
ZXR10_R4(config-if)#exit
ZXR10_R4(config)#interface vlan2
ZXR10_R4(config-if)#ip address 10.0.1.2 255.255.255.252
ZXR10_R4(config-if)#exit
ZXR10_R4(config)#router ospf 1
ZXR10_R4(config-router)#network 10.0.1.0 0.0.0.3 area 1
ZXR10_R4(config-router)#area 1 nssa
ZXR10_R4(config-router)#redistribute rip metric 10
```

Configuration on R5:

```
ZXR10_R5(config)#interface vlan1
ZXR10_R5(config-if)#ip address 10.0.2.2 255.255.255.252
ZXR10_R5(config-if)#exit
ZXR10_R5(config)#router ospf 1
ZXR10_R5(config-router)#network 10.0.2.0 0.0.0.3 area 2
ZXR10_R5(config-router)#area 2 stub
```

OSPF Virtual Link Configuration Example

[Figure 8](#) presents an example of configuring OSPF virtual link.

FIGURE 8 OSPF VIRTUAL LINK CONFIGURATION EXAMPLE**Configuration on R1:**

```
ZXR10_R1(config)#interface vlan1
ZXR10_R1(config-if)#ip address 10.0.0.1 255.255.255.0
ZXR10_R1(config-if)#exit
ZXR10_R1(config)#router ospf 1
ZXR10_R1(config-router)#network 10.0.0.0 0.0.0.255 area 0
```

Configuration on R2:

```
ZXR10_R2(config)#interface vlan1
ZXR10_R2(config-if)#ip address 10.0.0.2 255.255.255.0
ZXR10_R2(config-if)#exit
ZXR10_R2(config)#interface vlan2
ZXR10_R2(config-if)#ip address 10.0.1.1 255.255.255.252
ZXR10_R2(config-if)#exit
ZXR10_R2(config)#router ospf 1
ZXR10_R2(config-router)#network 10.0.0.0 0.0.0.255 area 0
ZXR10_R2(config-router)#network 10.0.1.0 0.0.0.3 area 1
ZXR10_R2(config-router)#area 1 virtual-link 10.0.1.2
```

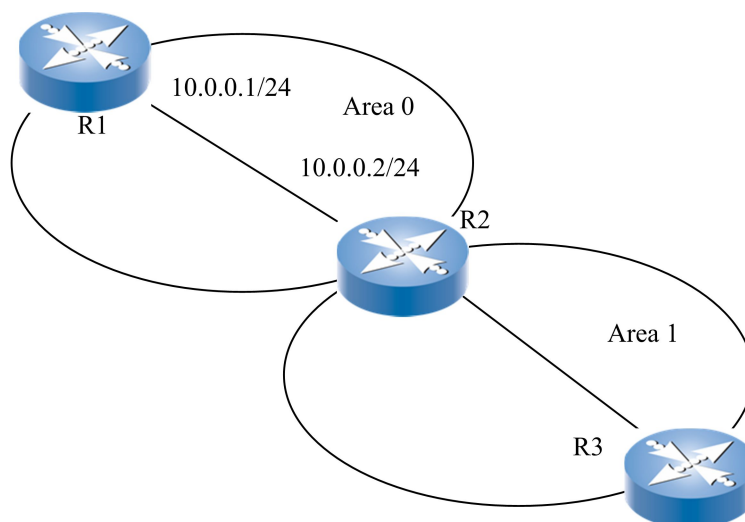
Configuration on R3:

```
ZXR10_R3(config)#interface vlan1
ZXR10_R3(config-if)#ip address 10.0.1.2 255.255.255.252
ZXR10_R3(config-if)#exit
ZXR10_R3(config)#interface vlan2
ZXR10_R3(config-if)#ip address 10.0.2.1 255.255.255.0
ZXR10_R3(config-if)#exit
ZXR10_R3(config)#router ospf 1
ZXR10_R3(config-router)#network 10.0.1.0 0.0.0.3 area 1
ZXR10_R3(config-router)#network 10.0.2.0 0.0.0.255 area 2
ZXR10_R3(config-router)#area 1 virtual-link 10.0.1.2
```

OSPF Authentication Configuration Example

Figure 9 presents an example of configuring OSPF authentication. Area 0 uses simple text authentication, and area 1 uses MD5 authentication.

FIGURE 9 OSPF AUTHENTICATION CONFIGURATION EXAMPLE



Configuration on R1:

```
ZXR10_R1(config)#interface vlan1
ZXR10_R1(config-if)#ip address 10.0.0.1 255.255.255.0
ZXR10_R1(config-if)#ip ospf authentication-key ZXR10
ZXR10_R1(config-if)#exit
ZXR10_R1(config)#router ospf 1
ZXR10_R1(config-router)#network 10.0.0.0 0.0.0.255 area 0
ZXR10_R1(config-router)#area 0 authentication
```

Configuration on R2:

```
ZXR10_R2(config)#interface vlan1
ZXR10_R2(config-if)#ip address 10.0.0.2 255.255.255.0
ZXR10_R2(config-if)#ip ospf authentication-key ZXR10
ZXR10_R2(config-if)#exit
ZXR10_R2(config)#interface vlan2
ZXR10_R2(config-if)#ip address 10.0.1.1 255.255.255.252
ZXR10_R2(config-if)#ip ospf message-digest-key 1 md5 ZXR10
ZXR10_R2(config-if)#exit
ZXR10_R2(config)#router ospf 1
ZXR10_R2(config-router)#network 10.0.0.0 0.0.0.255 area 0
ZXR10_R2(config-router)#network 10.0.1.0 0.0.0.3 area 1
ZXR10_R2(config-router)#area 0 authentication
ZXR10_R2(config-router)#area 1 authentication message-digest
```

Configuration on R3:

```
ZXR10_R3(config)#interface vlan1
ZXR10_R3(config-if)#ip address 10.0.1.2 255.255.255.252
ZXR10_R3(config-if)#ip ospf message-digest-key 1 md5 ZXR10
ZXR10_R3(config-if)#exit
ZXR10_R3(config)#router ospf 1
ZXR10_R3(config-router)#network 10.0.1.0 0.0.0.3 area 1
ZXR10_R3(config-router)#area 1 authentication message-digest
```

OSPF Maintenance and Diagnosis

To configure OSPF maintenance and diagnosis, perform the following steps.

Step	Command	Function
1	<code>ZXR10#show ip ospf [<process-id>]</code>	This views the detailed information of OSPF process
2	<code>ZXR10#show ip ospf interface [<interface-name>][process <process-id>]</code>	This views interface configuration information and state
3	<code>ZXR10#show ip ospf neighbor [interface <interface-name>][neighbor-id <neighbor>][process <process-id>]</code>	This views OSPF neighbor
4	<code>ZXR10#show ip ospf database</code>	This views link state database
5	<code>ZXR10#debug ip ospf adj</code>	This tracks OSPF adjacency information
6	<code>ZXR10#debug ip ospf packet</code>	This tracks OSPF receiving packets and sending packets
7	<code>ZXR10#debug ip ospf lsa-generation</code>	This tracks OSPF LSA generation information
8	<code>ZXR10#debug ip ospf events</code>	This tracks OSPF events



Note:

When two routers cannot communicate, it is because the adjacency is not formed. Check whether the neighbor relationship state between two OSPF routers is Full. Full state is the flag of normal running OSPF protocol.

Link state database is the source of all OSPF routes in the IP routing table. Many route problems may be caused by the incorrect information or information losing in the link state database.

IS-IS Configuration

Table of Contents

IS-IS Overview	35
Configuring IS-IS	37
IS-IS Configuration Examples.....	40
IS-IS Maintenance and Diagnosis.....	44

IS-IS Overview

Intermediate System-to-Intermediate System (**IS-IS**) is a routing protocol introduced by International Organization for Standardization (**ISO**) for Connectionless Network Service (**CLNS**). IS-IS works on the network layer of the Open Systems Interconnection (**OSI**). When IS-IS is expanded and added with the function to support IP routing, it becomes Integrated IS-IS. The IS-IS introduced in this document refers to Integrated IS-IS.

IS-IS protocol is widely used in network as an IGP. The working mechanism of IS-IS is similar to that of OSPF: Partition the network into areas, in which the router only manages the routing information in the area. This saves router cost. This feature enables IS-IS to be used to meet the requirements of large-scaled network.

IS-IS protocol is based on CLNS instead of IP. When the routers are communicating, IS-IS uses Protocol Data Unit (**PDU**) defined by ISO. There are three types of PDUs that are used in IS-IS:

- Hello PDU
- Link state PDU (LSP)
- Sequence number PDU (**SNP**)

Hello PDU is similar to Hello message in OSPF protocol. It is responsible for forming adjacency between routers. It is also used to find new neighbor and detect whether any neighbor exits.

IS-IS routers exchange routing information, set up and maintain link state database by use of link state PDUs. An LSP indicates important information about a router, covering area and connected network. SNP is used to ensure reliable transmission of LSPs. SNP contains summary information about each LSP on a network.

When a router receives an SNP, it compares SNP with link state database. If router loses an LSP in SNP, it originates a multicast SNP and asks for necessary LSPs from other routers on the network. LSPs are used in conjunction with SNPs so that IS-IS protocol can complete reliable route interaction on a large network.

IS-IS protocol also uses the Dijkstra SPF algorithm to calculate routes. Based on the link state database, IS-IS protocol uses the SPF algorithm to calculate the best route and then adds the route to the IP routing table.

IS-IS Area

For convenience of link-state database management, concept of IS-IS area is introduced. Routers in an area are only responsible for maintaining the link state database in the local area to reduce the traffic of the routers themselves.

IS-IS areas are classified into backbone areas and non-backbone areas:

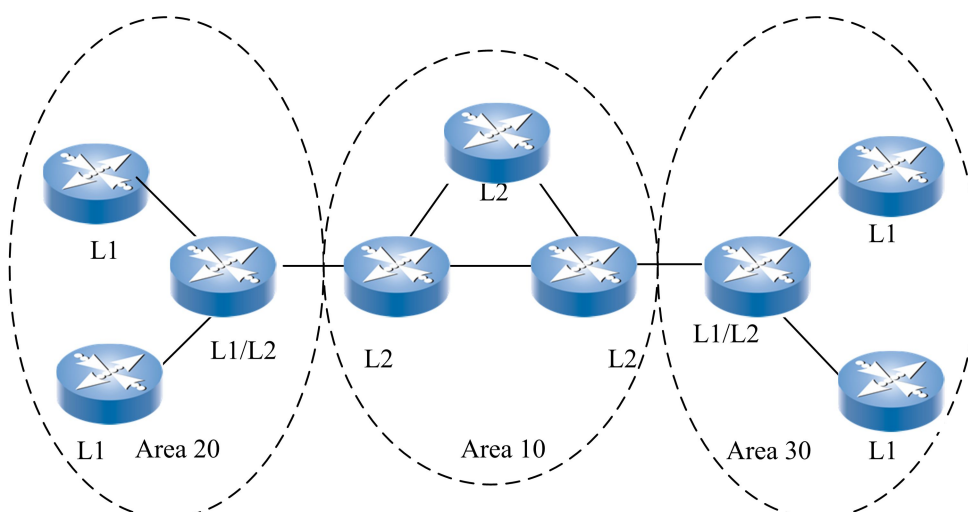
- Routers in the backbone area have the information about the database of the entire network.
- Routers in a non-backbone area only have information about the area.

Based on the area division, IS-IS defines three types of routers:

- L1 router exists in a non-backbone area and only exchanges routing information with L1 router and L1/L2 router in the area.
- L2 router exists in the backbone area and exchanges routing information with other L2 routers and L1/L2 routers.
- L1/L2 routers exist in a non-backbone area and exchanges routing information between non-backbone area and the backbone area.

IS-IS area division and router types are shown in [Figure 10](#).

FIGURE 10 IS-IS AREA



IS-IS Network Types

There are two types of IS-IS networks:

- Broadcast network
- Point-to-point networks

This makes it easier to configure and implement IS-IS.

DIS and Router Priority

In a broadcast network, IS-IS protocol is similar to OSPF protocol and uses designated router. **DIS** is responsible for advertising network information to all routers on the broadcast network. Only one of other routers will be advertised to DIS adjacency.

The router priority parameters can be IS-IS configured for DIS election. L1 and L2 can be configured with different priorities independently. Upon DIS election, a highest priority router plays the role of DIS.

If priorities are same for a frame relay interface, a router with higher system ID is elected as the DIS. While for an Ethernet interface, a router with higher interface MAC value is elected as the DIS.

Configuring IS-IS

Enabling IS-IS

To configure basic IS-IS, perform the following steps.

Step	Command	Function
1	ZXR10 (config) # router isis [vrf <vrf-name>]	This enables IS-IS process
2	ZXR10 (config-router) # area <area-address>	This configures IS-IS area
3	ZXR10 (config-router) # system-id <system-id> [range <range-number>]	This configures system ID
4	ZXR10 (config-router) # exit	This exits IS-IS route configuration mode
5	ZXR10 (config) # interface <interface-name>	This enters interface configuration mode
6	ZXR10 (config-if) # ip router isis	This specifies interface to run IS-IS

**Note:**

In IS-IS route configuration mode, it is required to define an area that the router belongs to. It is also required to define a system ID. System ID identifies the router in the area. It is indicated with the interface MAC address of the router. By default, the router running IS-IS protocol is identified as LEVEL-1-2. To optimize network, IS-IS area can be modified by the following command.

Configuring IS-IS Global Parameters

When configuring IS-IS on ZXR10 series switches or routers, use default parameter value. If the routers or switches are connecting with devices of other vendors, related interface parameters and timer may have to be adjusted. This makes IS-IS protocol run more efficiently in the network.

To set IS-IS global parameters, perform the following steps.

Step	Command	Function
1	<code>ZXR10(config)#router isis [vrf <vrf-name>]</code>	This enables IS-IS process
2	<code>ZXR10(config-router)#is-type {level-1 level-1-2 level-2-only}</code>	This sets IS-IS permitted level
3	<code>ZXR10(config-router)#set-overload-bit</code>	This advertises to other routers that are running IS-IS when the processing capability of the router is insufficient
4	<code>ZXR10(config-router)#default-information originate [always][metric <metric-value>][metric-type <type>][level-1 level-1-2 level-2]</code>	This configures default route advertisement policy
5	<code>ZXR10(config-router)#summary-address <ip-address><net-mask>[metric <metric-value>][level-1 level-1-2 level-2]</code>	This configures route aggregation

**Note:**

For step 4, when configuring route redistribution, redistribute default route in the routing entries to IS-IS domain.

For step 5, IS-IS can advertise outward an aggregation route instead of detailed route entries in routing table. The minimum metric in the aggregation route entries is selected as the metric of aggregation route.

Configuring IS-IS Interface Parameters

To set IS-IS interface parameters, perform the following steps.

Step	Command	Function
1	ZXR10 (config) # interface <interface-name>	This enters interface configuration mode
2	ZXR10 (config-if) # isis circuit-type { level-1 level-1-2 level-2-only }	This sets interface operation types
3	ZXR10 (config-if) # isis hello-interval <interval> [level-1 level-2]	This sets Hello packet interval
4	ZXR10 (config-if) # isis hello-multiplier <multiplier> [level-1 level-2]	This sets the multiple of interface keeping time and hello interval
5	ZXR10 (config-if) # isis lsp-interval <interval> [level-1 level-2]	This sets transmission interval of LSP packet
6	ZXR10 (config-if) # isis retransmit-interval <interval> [level-1 level-2]	This sets retransmission interval of LSP packet
7	ZXR10 (config-if) # isis priority <priority> [level-1 level-2]	This sets DIS election priority of interface
8	ZXR10 (config-if) # isis metric <metric-value> [level-1 level-2]	This sets IS-IS interface metric
9	ZXR10 (config-if) # isis csnp-interval <interval> [level-1 level-2]	This sets CSNP packet interval
10	ZXR10 (config-if) # isis psnp-interval <interval> [level-1 level-2]	This sets PSNP packet interval



Note:

For step 2, the value should match the IS-IS global operation type.

Command in step 8 is to set the metric when the interface participates IS-IS SPF calculation. Different metrics can be set for L1 and L2 at the same interface. The default value is 10.

For step 9, the default value is 10 in broadcast network. In the point-to-point network, the default value is 3600.

For step 10, PSNP is usually applied in point-to-point network. The parameter is used to set the transmission interval between two PSNPs, with default value of 3.

Configuring IS-IS Authentication

1. Setting Interface Authentication

Step	Command	Function
1	<code>ZXR10(config-if)#isis authentication <key>[level -1 level-2]</code>	This sets authentication key.
2	<code>ZXR10(config-if)#isis authentication-type {MD5 TEXT}[level-1 level-2]</code>	This sets interface authentication mode: MD5 authentication or simple password authentication.

2. Setting SNP Authentication

Step	Command	Function
1	<code>ZXR10(config-router)#authentication <key>[level-1 level-2]</code>	This sets authentication key.
2	<code>ZXR10(config-router)#enable-snp-authentication</code>	This sets SNP authentication.

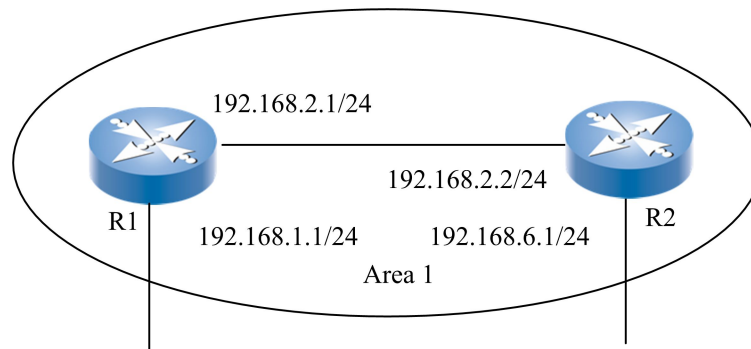
Example To configure SNP authentication with authentication string to be welcome, execute the following command:

```
ZXR10(config)#router isis
ZXR10(config-router)#authentication welcome
ZXR10(config-router)#enable-snp-authentication
```

IS-IS Configuration Examples

Single-Area IS-IS Configuration Example

This example describes how to configure the basic IS-IS, taking single-area network as an example, as shown in [Figure 11](#).

FIGURE 11 SINGLE-AREA IS-IS CONFIGURATION EXAMPLE

R1 and R2 form area 1, running IS-IS protocol.

Configuration on R1:

```
ZXR10_R1(config)#router isis
ZXR10_R1(config-router)#area 01
ZXR10_R1(config-router)#system-id 00D0.D0C7.53E0
ZXR10_R1(config-router)#exit
ZXR10_R1(config)#interface vlan4
ZXR10_R1(config-if)#ip address 192.168.2.1 255.255.255.0
ZXR10_R1(config-if)#ip router isis
ZXR10_R1(config)#interface vlan6
ZXR10_R1(config-if)#ip address 192.168.1.1 255.255.255.0
ZXR10_R1(config-if)#ip router isis
```

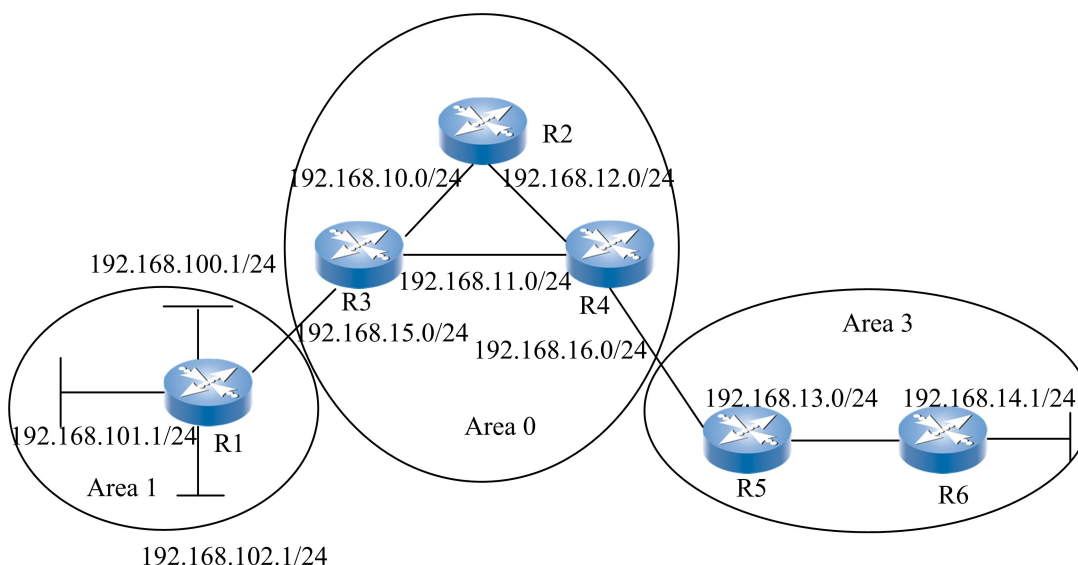
Configuration on R2:

```
ZXR10_R2(config)#router isis
ZXR10_R2(config-router)#area 01
ZXR10_R2(config-router)#system-id 00D0.D0C7.5460
ZXR10_R2(config-router)#exit
ZXR10_R2(config)#interface vlan4
ZXR10_R2(config-if)#ip address 192.168.2.2 255.255.255.0
ZXR10_R2(config-if)#ip router isis
ZXR10_R2(config)#interface vlan3
ZXR10_R2(config-if)#ip address 192.168.6.1 255.255.255.0
ZXR10_R2(config-if)#ip router isis
```

Multi-Area IS-IS Configuration Example

When the network is vast, use multiple areas in the IS-IS. Divide the similar routers into the same area according to the zone and functionality. Partition of area reduces memory requirement. It makes the router in an area maintain relatively smaller link state database. [Figure 12](#) is an example of configuring multi-area IS-IS.

FIGURE 12 MULTI-AREA IS-IS CONFIGURATION EXAMPLE



R1 belongs to area 1. R2, R3 and R4 belong to area 0. R5 and R6 belong to area 3. On R1, perform route aggregation to network segment in area 1. On R6, redistribute the default route to IS-IS.

Configuration on R1:

```
ZXR10_R1(config)#router isis
ZXR10_R1(config-router)#area 01
ZXR10_R1(config-router)#system-id 00D0.D0C7.53E0
ZXR10_R1(config-router)#is-type LEVEL-1-2
ZXR10_R1(config-router)#exit
ZXR10_R1(config)#interface vlan4
ZXR10_R1(config-if)#ip address 192.168.15.1 255.255.255.0
ZXR10_R1(config-if)#ip router isis
ZXR10_R1(config-if)#isis circuit-type LEVEL-2
ZXR10_R1(config-router)#exit
ZXR10_R1(config)#interface vlan6
ZXR10_R1(config-if)#ip address 192.168.100.1 255.255.255.0
ZXR10_R1(config-if)#ip router isis
ZXR10_R1(config-if)#isis circuit-type LEVEL-1
ZXR10_R1(config-if)#exit
ZXR10_R1(config)#interface vlan7
ZXR10_R1(config-if)#ip address 192.168.101.1 255.255.255.0
ZXR10_R1(config-if)#ip router isis
ZXR10_R1(config-if)#isis circuit-type LEVEL-1
ZXR10_R1(config-if)#exit
ZXR10_R1(config)#interface vlan8
ZXR10_R1(config-if)#ip address 192.168.102.1 255.255.255.0
ZXR10_R1(config-if)#ip router isis
ZXR10_R1(config-if)#isis circuit-type LEVEL-1
ZXR10_R1(config-if)#exit
ZXR10_R1(config)#router isis
ZXR10_R1(config-router)#summary-address 192.168.100.0
255.255.252.0 metric 10
```

Configuration on R2:

```
ZXR10_R2(config)#router isis
ZXR10_R2(config-router)#area 00
ZXR10_R2(config-router)#system-id 00D0.E0D7.53E0
ZXR10_R2(config-router)#is-type LEVEL-2
ZXR10_R2(config-router)#exit
ZXR10_R2(config)#interface vlan4
ZXR10_R2(config-if)#ip address 192.168.10.2 255.255.255.0
ZXR10_R2(config-if)#ip router isis
ZXR10_R2(config-if)#isis circuit-type LEVEL-2
```

```
ZXR10_R2(config-router)#exit
ZXR10_R2(config)#interface vlan6
ZXR10_R2(config-if)#ip address 192.168.12.2 255.255.255.0
ZXR10_R2(config-if)#ip router isis
ZXR10_R2(config-if)#isis circuit-type LEVEL-2
ZXR10_R2(config-if)#exit
```

Configuration on R3:

```
ZXR10_R3(config)#router isis
ZXR10_R3(config-router)#area 00
ZXR10_R3(config-router)#system-id 00D0.E0C7.53E0
ZXR10_R3(config-router)#is-type LEVEL-2
ZXR10_R3(config-router)#exit
ZXR10_R3(config)#interface vlan4
ZXR10_R3(config-if)#ip address 192.168.15.3 255.255.255.0
ZXR10_R3(config-if)#ip router isis
ZXR10_R3(config-if)#isis circuit-type LEVEL-2
ZXR10_R3(config-router)#exit
ZXR10_R3(config)#interface vlan6
ZXR10_R3(config-if)#ip address 192.168.10.3 255.255.255.0
ZXR10_R3(config-if)#ip router isis
ZXR10_R3(config-if)#isis circuit-type LEVEL-2
ZXR10_R3(config-if)#exit
ZXR10_R3(config)#interface vlan7
ZXR10_R3(config-if)#ip address 192.168.11.3 255.255.255.0
ZXR10_R3(config-if)#ip router isis
ZXR10_R3(config-if)#isis circuit-type LEVEL-2
ZXR10_R3(config-if)#exit
```

Configuration on R4:

```
ZXR10_R4(config)#router isis
ZXR10_R4(config-router)#area 00
ZXR10_R4(config-router)#system-id 00D0.E0E7.53E0
ZXR10_R4(config-router)#is-type LEVEL-2
ZXR10_R4(config-router)#exit
ZXR10_R4(config)#interface vlan4
ZXR10_R4(config-if)#ip address 192.168.12.4 255.255.255.0
ZXR10_R4(config-if)#ip router isis
ZXR10_R4(config-if)#isis circuit-type LEVEL-2
ZXR10_R4(config-router)#exit
ZXR10_R4(config)#interface vlan6
ZXR10_R4(config-if)#ip address 192.168.11.4 255.255.255.0
ZXR10_R4(config-if)#ip router isis
ZXR10_R4(config-if)#isis circuit-type LEVEL-2
ZXR10_R4(config-if)#exit
ZXR10_R4(config)#interface vlan7
ZXR10_R4(config-if)#ip address 192.168.16.4 255.255.255.0
ZXR10_R4(config-if)#ip router isis
ZXR10_R4(config-if)#isis circuit-type LEVEL-2
ZXR10_R4(config-if)#exit
```

Configuration on R5:

```
ZXR10_R5(config)#router isis
ZXR10_R5(config-router)#area 02
ZXR10_R5(config-router)#system-id 00D0.D0CF.53E0
ZXR10_R5(config-router)#is-type LEVEL-1-2
ZXR10_R5(config-router)#exit
ZXR10_R5(config)#interface vlan4
ZXR10_R5(config-if)#ip address 192.168.16.5 255.255.255.0
ZXR10_R5(config-if)#ip router isis
ZXR10_R5(config-if)#isis circuit-type LEVEL-2
ZXR10_R5(config-router)#exit
ZXR10_R5(config)#interface vlan6
ZXR10_R5(config-if)#ip address 192.168.13.5 255.255.255.0
ZXR10_R5(config-if)#ip router isis
ZXR10_R5(config-if)#isis circuit-type LEVEL-1
ZXR10_R5(config-if)#exit
```

Configuration on R6:

```

ZXR10_R6(config)#router isis
ZXR10_R6(config-router)#area 02
ZXR10_R6(config-router)#system-id 00D0.0ECD.53E0
ZXR10_R6(config-router)#is-type LEVEL-1
ZXR10_R6(config-router)#exit
ZXR10_R6(config)#interface vlan4
ZXR10_R6(config-if)#ip address 192.168.13.6 255.255.255.0
ZXR10_R6(config-if)#ip router isis
ZXR10_R6(config-if)#isis circuit-type LEVEL-1
ZXR10_R6(config-router)#exit
ZXR10_R6(config)#interface vlan8
ZXR10_R6(config-if)#ip address 192.168.14.1 255.255.255.0
ZXR10_R6(config-if)#exit
ZXR10_R6(config)#ip route 0.0.0.0 0.0.0.0 192.168.14.10
ZXR10_R6(config)#router isis
ZXR10_R6(config-router)#default-information originate
ZXR10_R6(config-router)#redistribute protocol static metric 10
ZXR10_R6(config-router)#end

```

IS-IS Maintenance and Diagnosis

To configure IS-IS maintenance and diagnosis, perform the following steps.

Step	Command	Function
1	ZXR10#show isis adjacency [level-1 level-2][vrf <vrf-name>]	This views neighbor state
2	ZXR10#show isis circuits [detail][vrf <vrf-name>]	This views interface information
3	ZXR10#show isis database [level-1 level-2][detail][vrf <vrf-name>]	This views current IS-IS database information
4	ZXR10#show isis topology [level-1 level-2][vrf <vrf-name>]	This views current IS-IS topology
5	ZXR10#debug isis adj-packets	This tracks hello message that IS-IS received and transmitted
6	ZXR10#debug isis snp-packets	This tracks SNP message that IS-IS received and transmitted
7	ZXR10#debug isis spf-events	This tracks IS-IS routing calculation event debugging information
8	ZXR10#debug isis update-packets	This tracks IS-IS LSP packet processing event debugging information

BGP Configuration

Table of Contents

BGP Overview	45
Configuring BGP	46
BGP Configuration Example	62
BGP Maintenance and Diagnosis	64

BGP Overview

Border Gateway Protocol ([BGP](#)) is an inter-domain routing protocol, exchanging Network Layer Reachable Information (NLRI) between [ASs](#) that run BGP. The information mainly includes the list of ASs that a route passes through, which can be used to compose an AS connection state diagram. This makes the AS-based routing policy possible and solves the loop problem.

BGP of version 4 (BGP4) is defined in RFC1771. BGP4 supports the implementation of [CIDR](#), supernet and subnet and the functions such as route aggregation and route filtering. At present, BGP4 is widely applied in Internet.

A session set up between BGP routers in different ASs is called an [EBGP](#) session, while a session established between BGP routers in the same AS is called an [IBGP](#) session. A management area that has its own independent routing policy is called an autonomous system (AS). An important feature of an AS is that from the perspective of another AS, it has a set of internal routes and shows identical topology for reachable destinations. The AS indicator is a 16-bit value ranging from 1 to 65535, where the numbers between 1 to 32767 can be allocated, those from 32768 to 64511 are reserved, and those from 64512 to 65535 are used for private ASs (similar to private network addresses in IP address).

The BGP is based on reliable transmission protocol, with the TCP as its bottom protocol and the TCP port as 179. The BGP routers firstly set up a TCP connection, and then exchange all routing table information after packet authentication. After that, when the routing table changes, they send route update packets to all BGP neighbors, who will further spread the routing information until it reaches the whole network.

When a router sends a BGP update packet regarding to the destination network to its peer, the packet contains BGP metric, which is called path attribute. The path attributes include four types:

1. Well-Known Mandatory Attributes: The attributes must be present in route description.
 - ▶ AS-path
 - ▶ Next-hop
 - ▶ Origin
2. Well-Known Discretionary Attributes: The attributes can be absent from route description.
 - ▶ Local preference
 - ▶ Atomic aggregate
3. Optional transitive attributes: This kind of attributes is not necessary to be supported by all BGP implementation. When supported, the attributes can be transmitted to the BGP neighbors; if not supported by the current router, the attributes need to be transmitted to other BGP routers.
 - ▶ Aggregator
 - ▶ Community
4. Optional nontransitive attributes: It indicates that the router not supporting this kind of attributes shall delete the attributes.

Besides the above attributes, the weight attribute (defined by CISCO) is also a common attribute.

When searching BGP route, switch adopts multiple recursive searching mode to improve efficiency.

Configuring BGP

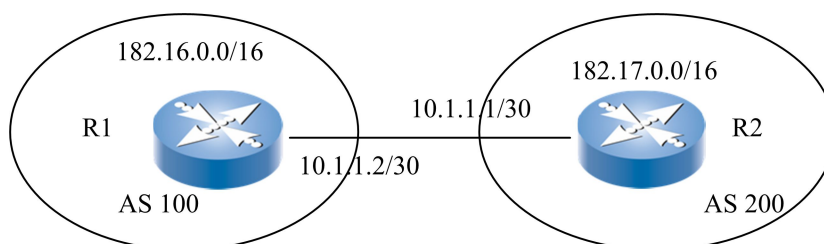
Enabling BGP

To enable BGP, perform the following steps.

Step	Command	Function
1	<code>ZXR10(config)#router bgp <as-number></code>	This starts BGP process
2	<code>ZXR10(config-router)#neighbor <ip-address> remote-as <number></code>	This sets BGP neighbor
3	<code>ZXR10(config-router)#network <ip-address><net-ma sk>[route-map <map-tag>]</code>	This advertises a network

Example [Figure 13](#) shows an example of BGP configuration. R1 resides in AS 100 and R2 resides in AS 200.

FIGURE 13 BASIC BGP CONFIGURATION



Configuration on R1:

```

ZXR10_R1(config)#router bgp 100
ZXR10_R1(config-router)#neighbor 10.1.1.1 remote-as 200
ZXR10_R1(config-router)#network 182.16.0.0 255.255.0.0
  
```

Configuration R2:

```

ZXR10_R2(config)#router bgp 200
ZXR10_R2(config-router)#neighbor 10.1.1.2 remote-as 100
ZXR10_R3(config-router)#network 182.17.0.0 255.255.0.0
  
```

In the configurations above, R1 and R2 define the other party as a BGP neighbor each other. Since R1 and R2 reside in different ASs, an EBGP session will be established. R1 will advertise network 182.16.0.0/16. R2 will advertise network 182.17.0.0/16.

Configuring BGP Route Advertisement

There are two methods to advertise BGP routes. One method is to use **network** command, the other is to use **redistribute** command.

To advertise a network, perform the following steps.

Step	Command	Function
1	ZXR10 (config) # router bgp <as-number>	This starts BGP process
2	ZXR10 (config-router) # network <ip-address> <net-mask> [route-map <map-tag>]	This advertises a network



Note:

Command in step 2 is used to advertise the networks known by the local router. Known networks include the networks that can be learnt by direct connections, static routes and dynamic routes.

To redistribute routes, perform the following steps.

Step	Command	Function
1	<code>ZXR10(config)#router bgp <as-number></code>	This starts BGP process
2	<code>ZXR10(config-router)#redistribute <protocol>[metric <metric-value>][route-map <map-tag>]</code>	This Redistributes the routes obtained by other routing protocols into the BGP routing table

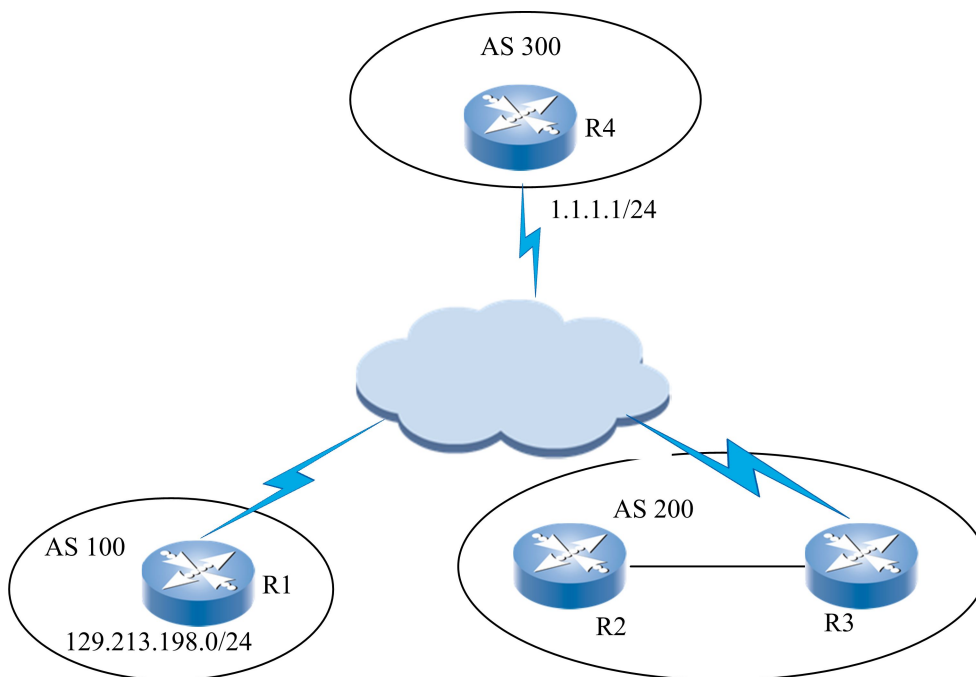
**Note:**

Command in step 2 is used to redistribute routes learnt by IGP protocols (RIP, OSPF, IS-IS) into BGP. When using this command, make sure that the routes learned by IGP from BGP are not redistributed into BGP. Use the filtering command to prevent the loop from occurring if necessary.

The route source of the static routes re-distributed into BGP is shown as "incomplete" in the routing table.

Example This example shows how to advertise routes in BGP by route re-distribution. Network topology is shown in [Figure 14](#).

FIGURE 14 BGP ROUTE ADVERTISEMENT CONFIGURATION

**Configuration on R3:**

```
ZXR10_R3(config)#router ospf 1
ZXR10_R3(config-router)#network 175.220.0.0 0.0.0.255 area 0
ZXR10_R3(config)#router bgp 200
ZXR10_R3(config-router)#neighbor 1.1.1.1 remote-as 300
ZXR10_R3(config-router)#redistribute ospf
```

Configuring BGP Route Aggregation

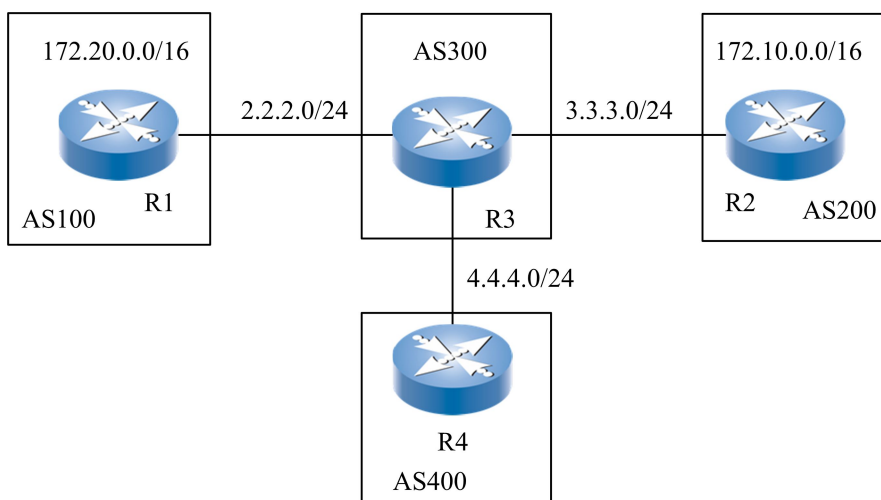
BGP can aggregate several pieces of learnt routing information into one piece and advertise it to the outside. This reduces the number of route entries in the routing table greatly.

To configure BGP route aggregation, perform the following steps.

Step	Command	Function
1	ZXR10(config)# router bgp <as-number>	This starts BGP process
2	ZXR10(config-router)# aggregate-address <ip-address><net-mask>[count <count>][as-set][summary-only][strict]	This advertises aggregated BGP routes

Example R1 and R2 advertise route 172.20.0.0/16 and 172.10.0.0/16 respectively, as shown in Figure 15. R3 aggregates the two pieces of routing information into 170.0.0.0/8 and advertises it to R4. After that, the R4 routing table can only learn the aggregated route 170.0.0.0/8.

FIGURE 15 BGP ROUTE AGGREGATION CONFIGURATION



Configuration on R1:

```

ZXR10_R1(config)#interface vlan1
ZXR10_R1(config-if)#ip address 2.2.2.2 255.255.255.0
ZXR10_R1(config)#router bgp 100
ZXR10_R1(config-router)#network 170.20.0.0 255.255.0.0
ZXR10_R1(config-router)#neighbor 2.2.2.1 remote-as 300
  
```

Configuration on R2:

```

ZXR10_R2(config)#interface vlan1
ZXR10_R2(config-if)#ip address 3.3.3.3 255.255.255.0
ZXR10_R2(config)#router bgp 200
ZXR10_R2(config-router)#network 170.10.0.0 255.255.0.0
ZXR10_R2(config-router)#neighbor 3.3.3.1 remote-as 300
  
```

Configuration on R3:

```

ZXR10_R3(config)#interface vlan1
ZXR10_R3(config-if)#ip address 2.2.2.1 255.255.255.0
ZXR10_R3(config)#interface vlan2
ZXR10_R3(config-if)#ip address 3.3.3.1 255.255.255.0
ZXR10_R3(config)#interface vlan3
ZXR10_R3(config-if)#ip address 4.4.4.1 255.255.255.0
ZXR10_R3(config)#router bgp 300
ZXR10_R3(config-router)#neighbor 2.2.2.2 remote-as 100
ZXR10_R3(config-router)#neighbor 3.3.3.3 remote-as 200
ZXR10_R3(config-router)#neighbor 4.4.4.4 remote-as 400
ZXR10_R3(config-router)#aggregate-address 170.0.0.0
255.0.0.0 summary-only

```

R3 has learnt routes 170.20.0.0 and 170.10.0.0, but it advertises aggregate route 170.0.0.0/8 only. Pay attention to the **summary-only** keyword in the aggregate advertisement commands. If the parameter is not included, R3 will advertise the specific routes in addition to the aggregate route.

Configuration on R4:

```

ZXR10_R4(config)#interface vlan1
ZXR10_R4(config-if)#ip address 4.4.4.4 255.255.255.0
ZXR10_R4(config)#router bgp 400
ZXR10_R4(config-router)#neighbor 4.4.4.1 remote-as 300

```

Configuring EBGp Multi-Hop

Usually, EBGp neighbor is established on the direct-connect interfaces of two routers. To establish EBGp neighborhood on non-direct connect interfaces, the following commands shall be used to perform EBGp multihop configuration, as well as proper IGP or static route configuration to enable intercommunication between non-direct connect neighbors.

Command	Function
ZXR10(config-router)# neighbor <ip-address> ebgp-multihop [ttl <value>]	This configures EBGp multi-hop.

Example As shown in [Figure 16](#), to establish neighborhood between R1 and the non-direct connected interface (IP address is 180.225.11.1) on R2, it needs to set EBGp multi-hop.

FIGURE 16 EBGp MULTI-HOP CONFIGURATION

Configuration of R1:

```

ZXR10_R1(config)#router bgp 100 ZXR10_R1(config-router)#neighbor
180.225.11.1 remote-as 300 ZXR10_R1(config-router)#neighbor
180.225.11.1 ebgp-multihop

```

Configuration of R2:

```

ZXR10_R2(config)#router bgp 300 ZXR10_R2(config-router)#neighbor
129.213.1.2 remote-as 100

```

Filtering Routes through Route Map

Route filtering and attribute setting are the basis of BGP route selection. Input or output route attributes can be controlled as required by route filtering.

Route map is used to control routing information and re-distribute routes between route domains based on defined conditions. Route map usually determines route selections with the use of route attributes.

To filter routes through route map, perform the following steps.

Step	Command	Function
1	ZXR10 (config) # router bgp <as-number>	This starts BGP process
2	ZXR10 (config-router) # neighbor <ip-address> route-map <map-tag> {in out}	This configures filtration of routes advertised by or to the neighbors
3	ZXR10 (config-router) # route-map <map-tag> [permit deny] [<sequence-number>]	This defines a route map

Example This example shows how to filter routes through route map.

```
ZXR10_R1(config)#router bgp 100
ZXR10_R1(config-router)#neighbor 182.17.20.1 remote-as 200
ZXR10_R1(config-router)#neighbor 182.17.20.1 route-map MAP1 out
ZXR10_R1(config-router)#neighbor 182.17.20.1 send-med
ZXR10_R1(config)#route-map MAP1 permit 10
ZXR10_R1(config-route-map)#match ip address 1
ZXR10_R1(config-route-map)#set metric 5
ZXR10_R1(config)#acl standard number 1
ZXR10_R1(config-std-acl)#rule 1 permit 172.3.0.0 0.0.255.255
```

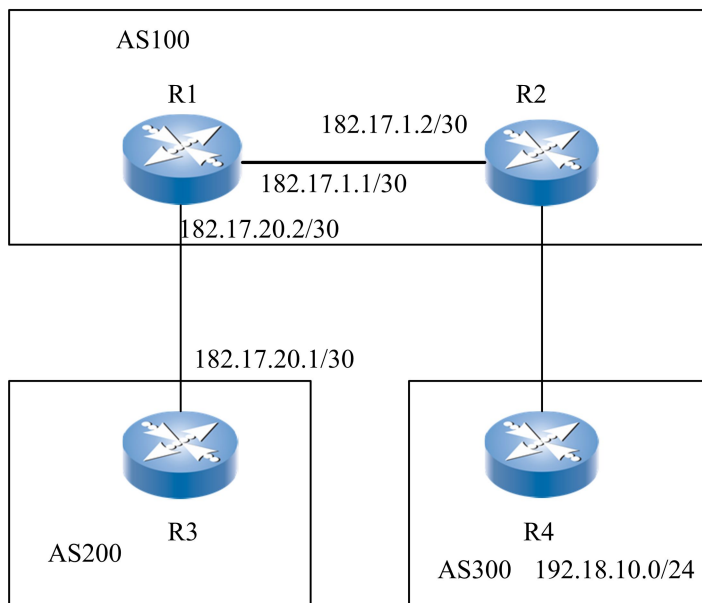
The above configuration defines a route map MAP1, which allows network 172.3.0.0 to be advertised to autonomous system 200 and sets the MED value to 5. When filtering routes through route map, **match** and **set** commands are both usually used. The **match** command defines matching criteria. The **set** command defines actions to be executed when the match conditions are satisfied.

Filtering Routes through NLRI

To restrict a router from obtaining or advertising routing information, route updates from or to a special neighbor device can be filtered. A filter contains an update list from or to a neighbor router.

Example As shown in [Figure 17](#), R1 and R2 are mutually IBGP peers, R1 and R3 are mutually EBGP peers, and R4 and R2 are mutually EBGP peers.

FIGURE 17 FILTERING ROUTES THROUGH NLRI



To prevent AS100 from playing the role of a transitional AS, the network 192.18.10.0/24 from AS300 can be advertised to AS200. R1 is configured with filtering function as follows:

```

ZXR10_R1(config)#router bgp 100
ZXR10_R1(config-router)#no synchronization
ZXR10_R1(config-router)#neighbor 182.17.1.2 remote-as 100
ZXR10_R1(config-router)#neighbor 182.17.20.1 remote-as 200
ZXR10_R1(config-router)#neighbor 182.17.20.1 route-map MAP1 out
ZXR10_R1(config)#route-map MAP1 permit 10
ZXR10_R1(config-route-map)#match ip address 1
ZXR10_R1(config)#access-list 1 deny 192.18.10.0 0.0.0.255
ZXR10_R1(config)#access-list 1 permit 0.0.0.0 255.255.255.255
  
```

In this example, the **route-map** command and the access control list are used to prevent R1 from advertising prefix 192.18.10.0/24 to AS200.

Filtering Routes through AS_PATH Attribute

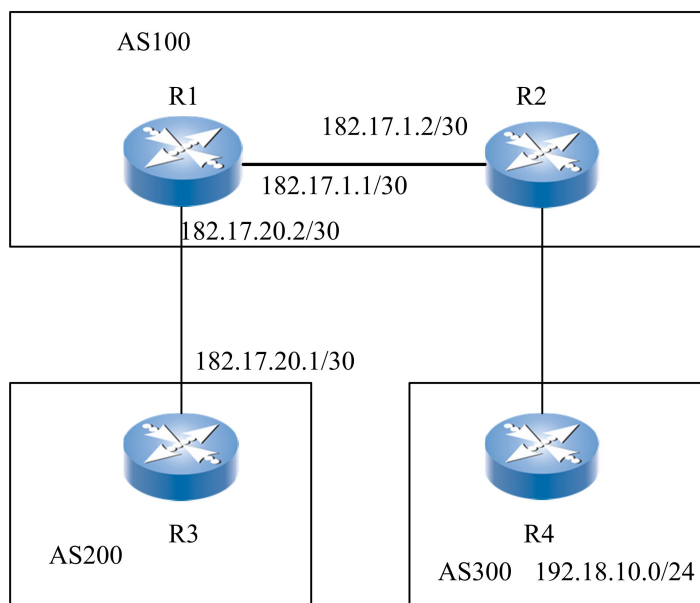
When all routes in one or more ASs are to be filtered, use filtration method based on AS path information. This prevents it from being complex due to prefix-based filtering.

To filter routes through AS_PATH attribute, use the following command.

Command	Function
<code>ZXR10(config)#ip as-path access-list <access-list-number> >{permit deny}<as-regular-expression></code>	This rules an access list for input and output based on the AS route attribute

Example R1 and R2 are IBGP peers of each other. R1 and R3 are EBGP peers of each other. R2 and R4 are EBGP peers of each other. Network topology is shown in Figure 18. Routes are filtered based on AS path, which prevents R1 from advertising network 192.18.10.0/24 (coming from AS300) to AS200.

FIGURE 18 FILTERING ROUTES THROUGH AS_PATH ATTRIBUTE



Configuration on R1:

```

ZXR10_R1(config)#router bgp 100
ZXR10_R1(config-router)#no synchronization
ZXR10_R1(config-router)#neighbor 182.17.1.2 remote-as 100
ZXR10_R1(config-router)#neighbor 182.17.20.1 remote-as 200
ZXR10_R1(config-router)#neighbor 182.17.20.1 route-map MAP1 out
ZXR10_R1(config)#route-map MAP1 permit 10
ZXR10_R1(config-route-map)#match as-path 1
ZXR10_R1(config)#ip as-path access-list 1 permit ^100$
  
```

In the above configuration, the AS ACL allows R1 to advertise the networks initiated from AS100 only to AS200, thus filtering network 192.18.10.0/24.

Configuring LOCAL_PREF Attribute

LOCAL_PREF attribute is used to determine the route selection between IBGP peers within an AS.

When two IBGP routers in an AS have learnt a route with the same destination from the outside, LOCAL_PREF attribute values are compared. The route with the higher value is preferred.

To configure LOCAL_PREF attribute, perform the following steps.

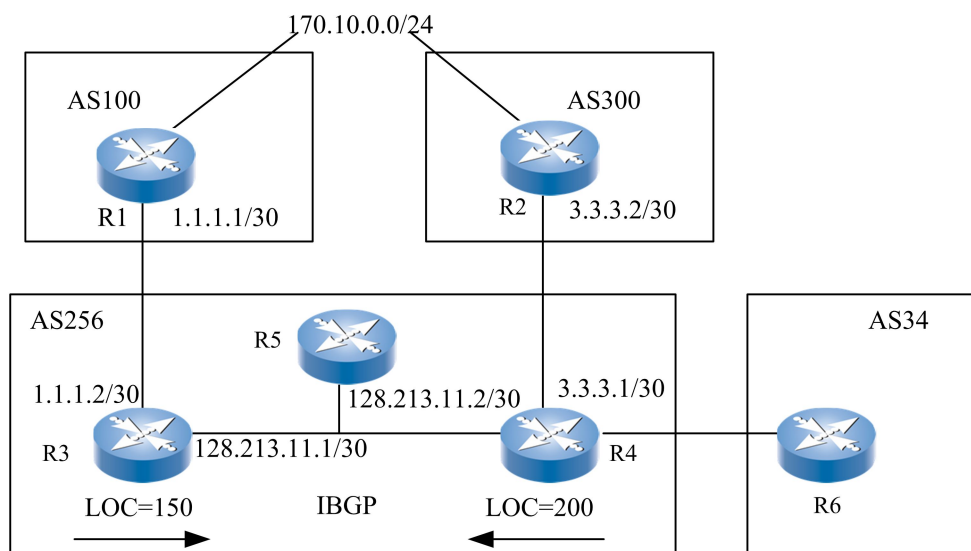
Step	Command	Function
1	<code>ZXR10(config)#router bgp <as-number></code>	This starts BGP process
2	<code>ZXR10(config-router)#bgp default local-preference <value></code>	This configures LOCAL_PREF attribute

**Note:**

The default value of LOCAL_PREF attribute is 100.

Example As shown in [Figure 19](#), R3 and R4 have learnt route to 170.10.0.0 at the same time. As LOCAL_PREF attribute value set for R4 is greater than that for R3, R4 egress is preferred for route to destination within AS256.

FIGURE 19 LOCAL_PREF ATTRIBUTE CONFIGURATION



Configuration on R3:

```
ZXR10_R3(config)#router bgp 256
ZXR10_R3(config-router)#neighbor 1.1.1.1 remote-as 100
ZXR10_R3(config-router)#neighbor 128.213.11.2 remote-as 256
ZXR10_R3(config-router)#bgp default local-preference 150
```

Configuration on R4:

```
ZXR10_R4(config)#router bgp 256
ZXR10_R4(config-router)#neighbor 3.3.3.2 remote-as 300
ZXR10_R4(config-router)#neighbor 128.213.11.1 remote-as 256
ZXR10_R4(config-router)#bgp default local-preference 200
```

Configuring MED Attribute

MED attribute is used for the interaction among ASs for route selection.

By default, the router only compares the metric values of the BGP neighbors in the same AS.

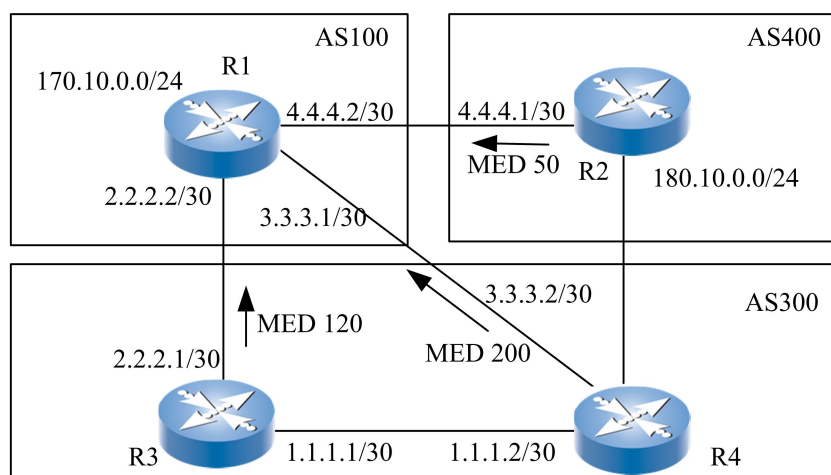
Default value of medic is 0. The path with a lower metric is preferred over a path with a higher metric. The metric value is not transferred to third-party ASs. That is, when an update packet with a metric value is received and it has to be transmitted to a third-party AS, the default metric value is transmitted.

To configure MED attribute, perform the following steps.

Step	Command	Function
1	ZXR10 (config) # router bgp <as-number>	This starts BGP process
2	ZXR10 (config-router) # neighbor <ip-address> send-med	This sends MED attribute to neighbor when advertising route
3	ZXR10 (config-route-map) # set metric <value>	This configures metric value
4	ZXR10 (config-router) # bgp always-compare-med	This compare metric values of the neighbors in different ASs

Example R1 receives the update of 180.10.0.0 from R2, R3 and R4 at the same time, as shown in [Figure 20](#). By default, only the metric values of neighbor R3 and R4 in the same AS are compared. The metric value of R3 is lower than that of R4, so R1 takes update packet from R3.

FIGURE 20 MED ATTRIBUTE CONFIGURATION



Configuration on R1:

```
ZXR10_R1(config)#router bgp 100
ZXR10_R1(config-router)#neighbor 2.2.2.1 remote-as 300
ZXR10_R1(config-router)#neighbor 3.3.3.2 remote-as 400
```

```
ZXR10_R1(config-router)#neighbor 4.4.4.1 remote-as 400
....
```

Configuration on R3:

```
ZXR10_R3(config)#router bgp 300
ZXR10_R3(config-router)#neighbor 2.2.2.2 remote-as 100
ZXR10_R3(config-router)#neighbor 2.2.2.2 route-map setmetricout out
ZXR10_R3(config-router)#neighbor 2.2.2.2 send-med
ZXR10_R3(config-router)#neighbor 1.1.1.2 remote-as 400
ZXR10_R3(config)#route-map setmetricout permit 10
ZXR10_R3(config-route-map)#set metric 120
```

Configuration on R4:

```
ZXR10_R4(config)#router bgp 300
ZXR10_R4(config-router)#neighbor 3.3.3.1 remote-as 100
ZXR10_R4(config-router)#neighbor 3.3.3.1 route-map setmetricout out
ZXR10_R4(config-router)#neighbor 3.3.3.1 send-med
ZXR10_R4(config-router)#neighbor 1.1.1.1 remote-as 400
ZXR10_R4(config)#route-map setmetricout permit 10
ZXR10_R4(config-route-map)#set metric 200
```

Configuration on R2:

```
ZXR10_R2(config)#router bgp 400
ZXR10_R2(config-router)#neighbor 4.4.4.2 remote-as 100
ZXR10_R2(config-router)#neighbor 4.4.4.2 route-map setmetricout out
ZXR10_R2(config-router)#neighbor 4.4.4.2 send-med
ZXR10_R2(config)#route-map setmetricout permit 10
ZXR10_R2(config-route-map)#set metric 50
```

Example In this example, the **bgp always-compare-med** command is used to allow a mandatory comparison of R1 metric value and R2 metric value. The metric value of R2 is lower than that of R3, so R1 will select R2 instead of R3 for the update of 180.10.0.0.

Configuration on R1:

```
ZXR10_R1(config)#router bgp 100
ZXR10_R1(config-router)#neighbor 2.2.2.1 remote-as 300
ZXR10_R1(config-router)#neighbor 3.3.3.2 remote-as 400
ZXR10_R1(config-router)#neighbor 4.4.4.1 remote-as 400
ZXR10_R1(config-router)#bgp always-compare-med
```

Configuring Community String Attribute

Community string is an optional transit attribute, ranging from 0~4,294,967,295. A selection can be made from a group of routes according to community attribute.

There are some definitions of the well-known community attributes, as shown below:

- No-export: Do not advertise this route to an EBGp neighbor.
- No-advertise: Do not advertise this route to any BGP neighbor.
- No-export-subconfed: Do not advertise the routes with this attribute to peers outside the confederation.

To configure community attribute, perform the following steps.

Step	Command	Function
1	ZXR10 (config) # router bgp <as-number>	This starts BGP process
2	ZXR10 (config-router) # neighbor <ip-address> send-community	This sends community attribute when advertising routes to neighbors

**Note:**

Community attribute is not sent to neighbors by default. Use **route-map** command to define community attribute when configuring community attribute.

Example In this example, R1 notifies its neighbors that route 192.166.1.0/24 should not be advertised to other EBGP neighbors.

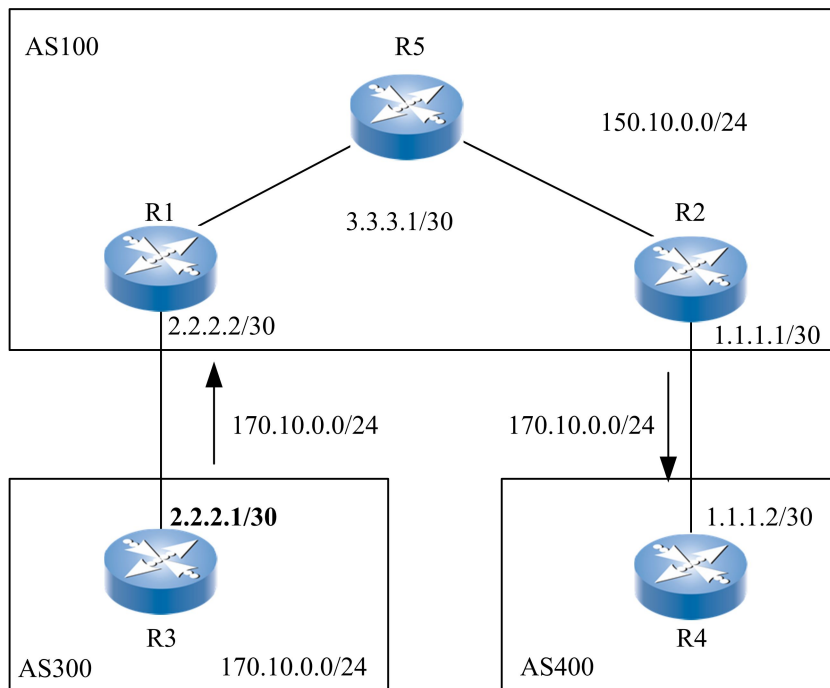
Configuration on R1:

```
ZXR10_R1(config)#router bgp 100
ZXR10_R1(config-router)#neighbor 3.3.3.3 remote-as 300
ZXR10_R1(config-router)#neighbor 3.3.3.3 send-community
ZXR10_R1(config-router)#neighbor 3.3.3.3 route-map setcommunity out
ZXR10_R1(config)#route-map setcommunity permit 10
ZXR10_R1(config-route-map)#match ip address 1
ZXR10_R1(config-route-map)#set community no-export
ZXR10_R1(config)#route-map setcommunity permit 20
ZXR10_R1(config)#acl standard number 1
ZXR10_R1(config-std-acl)#rule 1 permit 192.166.1.0 0.0.0.255
```

Configuring BGP Synchronization

As shown in [Figure 21](#), R1 and R2 run BGP. R1, R2 and R5 run OSPF.

FIGURE 21 CONFIGURING BGP SYNCHRONIZATION



R1 learns a route to 170.10.0.0 from AS 300. It advertises this route to R2 through IBGP connection.

Principle of BGP synchronization is: when a router advertises a route that is learnt from IBGP peer to a BGP peer, or adds this route to IGP routing table, there must be an IGP route from this route to the destination.

According to principle of BGP synchronization, R2 does not advertise the route that is learnt from R1 to R4. It is because there is no route from R2 to 170.10.0.0 in IGP routing table.

There are two ways to solve this problem:

1. Redistribute BGP routes on R1 or R2 into OSPF.
2. Run IBGP on R5 and make R1 and R2 full-connected. Then disables BGP synchronization on these three routers.

To disable BGP synchronization, use the following command.

Command	Function
ZXR10 (config-router) #no synchronization	This disables BGP synchronization.



Note:

By default, BGP synchronization is enabled.

Example This example shows how to disable BGP synchronization on R2 in [Figure 21](#).

```
ZXR10_R2 (config) #router bgp 100
```

```
ZXR10_R2(config-router)#no synchronization
```

Configuring BGP Route Reflector

For the BGP routers within the same AS, the neighbor relation should be established between every two routers to enable an overall interconnection. In this way, the number of neighbors increases to $n*(n-1)/2$ ("n" is the number of IBGP routers). Route reflector and confederation are used to reduce the workload of maintenance and configuration.

For IBGP speaking routers within an AS, one of them is selected to be the route reflector (RR). All the other IBGP routers act as clients and establish neighbor relation only with the RR. All the clients reflect routes by RR. This reduces the number of neighbors to $n-1$.

When a route is received by the RR, it is reflected depending on the type of peer.

- A route from a Non-Client peer is reflected to all Client peers.
- A route from a Client peer is reflected to all Non-Client peers and Client peers.
- A route from an EBGP peer is reflected to all Non-Client peers and Client peers.

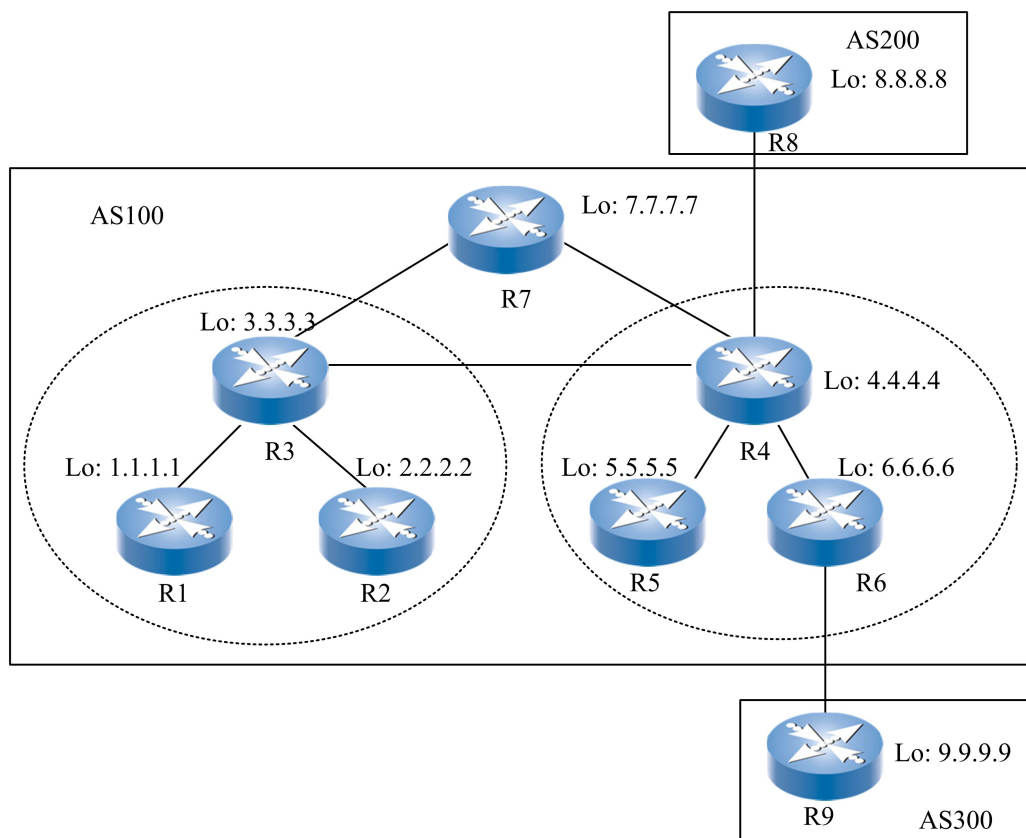
When there are multiple RRs in an AS, these RRs can be grouped into a cluster. An AS can include multi clusters. A cluster includes more than one RR at least.

To configure BGP route reflector, perform the following steps.

Step	Command	Function
1	<code>ZXR10(config)#router bgp <as-number></code>	This starts BGP process
2	<code>ZXR10(config-router)#neighbor <ip-address> router-reflector-client</code>	This configures BGP route reflector

Example R3 and R4 are two route reflectors in AS100. The clients of R4 are R5 and R6. The clients of R3 are R1 and R2. Network topology is shown in [Figure 22](#).

FIGURE 22 BGP ROUTE REFLECTOR



Configuration on R3:

```
ZXR10_R3(config)#router bgp 100
ZXR10_R3(config-router)#neighbor 2.2.2.2 remote-as 100
ZXR10_R3(config-router)#neighbor 2.2.2.2 route-reflector-client
ZXR10_R3(config-router)#neighbor 1.1.1.1 remote-as 100
ZXR10_R3(config-router)#neighbor 1.1.1.1 route-reflector-client
ZXR10_R3(config-router)#neighbor 7.7.7.7 remote-as 100
ZXR10_R3(config-router)#neighbor 4.4.4.4 remote-as 100
```

Configuration on R2:

```
ZXR10_R2(config)#router bgp 100
ZXR10_R2(config-router)#neighbor 3.3.3.3 remote-as 100
```

Configuring BGP Confederation

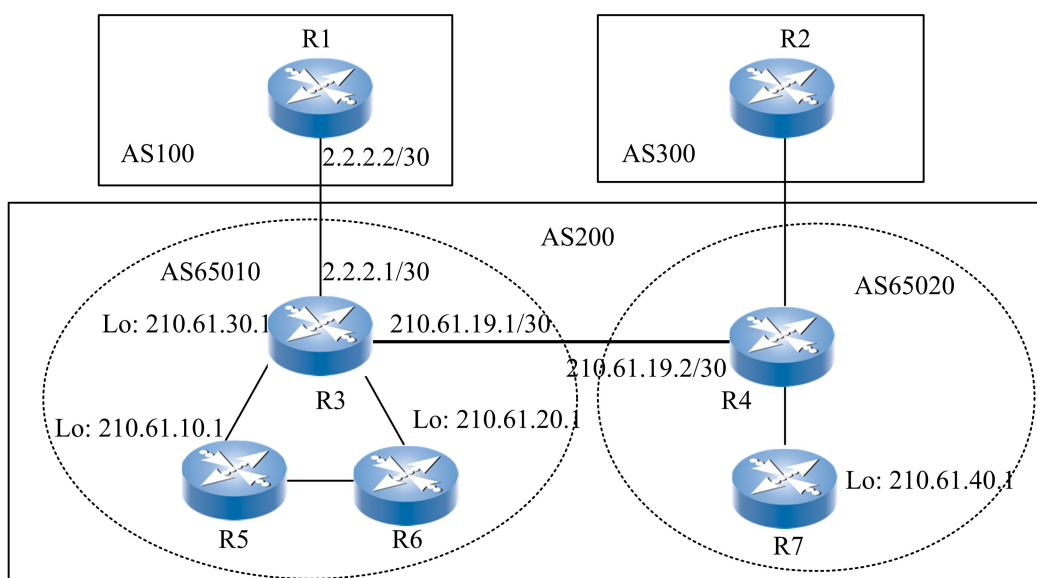
Route confederation has the similar function as the route reflector. It is to reduce the number of IBGP neighbor connections in an AS. Route confederation allows an AS to be divided into multi sub-ASs. IBGP routers in the AS belong to the sub-ASs respectively. IBGP is established within the sub-ASs. EBGP is established between the sub-ASs. The sub-AS ID is called confederation ID. Sub-ASs are invisible to the outside world of the AS.

To configure BGP confederation, perform the following steps.

Step	Command	Function
1	ZXR10 (config) # router bgp <as-number>	This starts BGP process
2	ZXR10 (config-router) # bgp confederation identifier <value>	This sets confederation ID
3	ZXR10 (config-router) # bgp confederation peers <value>[<value>]	This sets AS ID of a confederation peer

Example There are five BGP routers in AS200, as shown in [Figure 23](#). It is divided into two sub-ASs. One is defined as AS65010, which includes R3, R5 and R6, and the other is defined as AS65020, which includes R4 and R7.

FIGURE 23 BGP CONFEDERATION



Configuration on R3:

```
ZXR10_R3(config)#router bgp 65010
ZXR10_R3(config-router)#bgp confederation identifier 200
ZXR10_R3(config-router)#bgp confederation peers 65020
ZXR10_R3(config-router)#neighbor 210.61.10.1 remote-as 65010
ZXR10_R3(config-router)#neighbor 210.61.20.1 remote-as 65010
ZXR10_R3(config-router)#neighbor 210.61.19.2 remote-as 65020
ZXR10_R3(config-router)#neighbor 2.2.2.2 remote-as 100
```

Configuration on R5:

```
ZXR10_R5(config)#router bgp 65010
ZXR10_R5(config-router)#bgp confederation identifier 200
ZXR10_R5(config-router)#neighbor 210.61.30.1 remote-as 65010
ZXR10_R5(config-router)#neighbor 210.61.20.1 remote-as 65010
```

When establishing neighbor relation, EBGP neighbor relation is established between R3 and the confederation peers. IBGP neighbor relation is established with the confederation, and the EBGP neighbor relation is also established with AS100. The confederation is non-existent to AS100, so AS100 still establishes neighbor relation with R3 as AS200.

Configuration on R1:

```
ZXR10_R1(config)#router bgp 100
ZXR10_R1(config-router)#neighbor 2.2.2.1 remote-as 200
```

Configuring BGP Route Dampening

BGP provides route dampening mechanism to minimize the instability due to route flapping.

A route is assigned a penalty of 1000 per flap. When the penalty reaches a suppress-limit, the router stops advertising the route. The penalty decreases geometrically after every half-life-time. If the penalty decreases and falls below the reuse limit, the route is unsuppressed.

To configure BGP route dampening, perform the following steps.

Step	Command	Function
1	<code>ZXR10(config)#router bgp <as-number></code>	This starts BGP process
2	<code>ZXR10(config-router)#bgp dampening [<half-life><reuse><suppress><max-suppress-time>][<route-map><map-tag>]</code>	This configures BGP route dampening



Note:

Parameters are described below.

- *half-life*: ranging 1~45 minutes, 15 minutes by default.
- *reuse*: ranging 1~20000, 750 by default.
- *suppress*: ranging 1~20000, 2000 by default.
- *max-suppress*: ranging 1~255, 4 times of half-life-time by default.

Example This example shows how to enable dampening on a router.

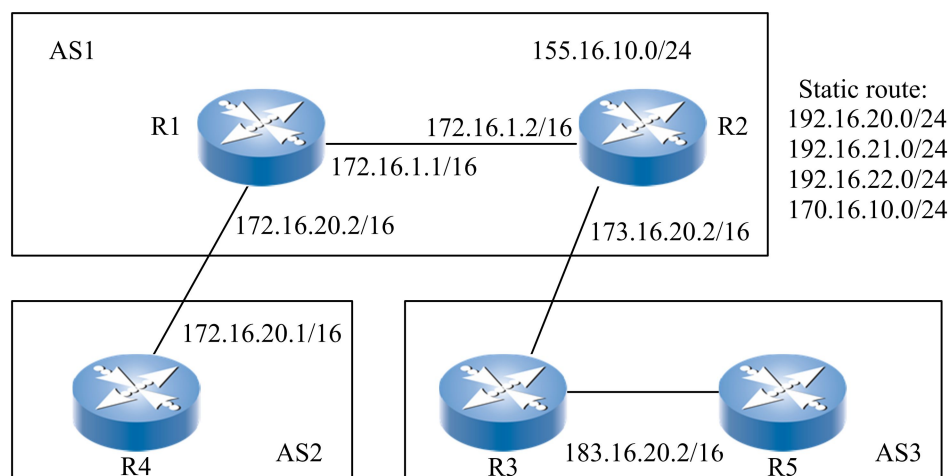
```
ZXR10(config)#router bgp 100
ZXR10(config-router)#bgp dampening
ZXR10(config-router)#network 203.250.15.0 255.255.255.0
ZXR10(config-router)#neighbor 192.208.10.5 remote-as 300
```

BGP Configuration Example

The following BGP example involves practical applications of BGP functions, including route aggregation and static route redistribution.

As shown in Figure 24, EBGP is established between R4 and R1. IBGP is established between R1 and R2. Multi-hop EBGP is established between R2 and R5. Suppose 4 static routes exist in R4. In R4 configuration, only 192.16.0.0/16 is aggregated and advertised. 170.16.10.0/24 is not allowed to be advertised through BGP to the outside world through route map. Multi-hop relation is established between R2 and R5 through R3. 155.16.10.0/24 is not allowed to be advertised through EBGP to the inside of R2 through route map. Make sure the neighbor addresses of the two routers are interconnected before configuring BGP.

FIGURE 24 BGP CONFIGURATION EXAMPLE



Configuration on R4:

```
ZXR10_R4(config)#router bgp 2
ZXR10_R4(config-router)#redistribute static
ZXR10_R4(config-router)#neighbor 172.16.20.2 remote-as 1
ZXR10_R4(config-router)#aggregate-address 192.16.0.0 255.255.0.0
count 0 as-set summary-only
ZXR10_R4(config-router)#neighbor 172.16.20.2 route-map torouter1 out
ZXR10_R4(config)#acl standard number 1
ZXR10_R4(config-std-acl)#rule 1 permit 172.16.10.0 0.0.0.255
ZXR10_R4(config)#route-map torouter1 deny 10
ZXR10_R4(config-route-map)#match ip address 1
ZXR10_R4(config)#route-map torouter1 permit 20
```

Configuration on R1:

```
ZXR10_R1(config)#route bgp 1
ZXR10_R1(config-router)#no synchronization
ZXR10_R1(config-router)#neighbor 172.16.1.2 remote-as 1
ZXR10_R1(config-router)#neighbor 172.16.1.2 next-hop-self
ZXR10_R1(config-router)#neighbor 172.16.20.1 remote-as 2
```

Configuration on R2:

```
ZXR10_R2(config)#ip route 183.16.0.0 255.255.0.0 vlan4
ZXR10_R2(config)#route bgp 1
ZXR10_R2(config-router)#neighbor 172.16.1.1 remote-as 1
ZXR10_R2(config-router)#neighbor 172.16.1.1 next-hop-self
ZXR10_R2(config-router)#neighbor 183.16.20.2 remote-as 3
ZXR10_R2(config-router)#neighbor 183.16.20.2 ebgp-multihop 2
ZXR10_R2(config-router)#neighbor 183.16.20.2 route-map torouter5 in
ZXR10_R2(config)#acl standard number 1
ZXR10_R2(config-std-acl)#rule 1 permit 155.16.10.0 0.0.0.255
ZXR10_R2(config)#route-map torouter5 deny 10
ZXR10_R2(config-route-map)#match ip address 1
ZXR10_R2(config)#route-map torouter5 permit 20
```

Configuration on R5:

```

ZXR10_R5(config)#ip route 173.16.0.0 255.255.0.0 gei_1/1
ZXR10_R5(config)#route bgp 3
ZXR10_R5(config-router)#neighbor 173.16.20.2 remote-as 1
ZXR10_R5(config-router)#neighbor 173.16.20.2 ebgp-multihop 2

```

BGP Maintenance and Diagnosis

To configure BGP maintenance and diagnosis, perform the following steps.

Step	Command	Function
1	ZXR10# show ip bgp protocol	This views BGP configuration information
2	ZXR10# show ip bgp neighbor	This views BGP neighbor information
3	ZXR10# show ip bgp route [network <ip-address>[mask <net-mask>]]	This views entries in BGP routing table
4	ZXR10# show ip bgp summary	This views states of BGP neighbor connections
5	ZXR10# debug ip bgp in	This tracks notification messages received by BGP and lists error codes and sub-error codes
6	ZXR10# debug ip bgp out	This tracks the notification messages sent by BGP and lists error codes and sub-error codes
7	ZXR10# debug ip bgp events	This tracks the BGP connecting statuses and migration

Example This example shows how to track the process of BGP state migration.

```

ZXR10#debug ip bgp events
BGP events debugging is on
ZXR10#
04:10:07: BGP: 192.168.1.2 reset due to Erroneous BGP Open received
04:10:07: BGP: 192.168.1.2 went from Connect to Idle
04:10:08: BGP: 192.168.1.2 went from Idle to Connect
04:10:13: BGP: 192.168.1.2 went from Connect to OpenSent
04:10:13: BGP: 192.168.1.2 went from OpenSent to OpenConfirm
04:10:13: BGP: 192.168.1.2 went from OpenConfirm to Established
ZXR10#

```

Load Sharing Configuration

Table of Contents

Load Sharing Overview.....	65
Configuring Load Sharing	66
Load Sharing Configuration Examples.....	66
Load Sharing Maintenance and Diagnosis.....	68

Load Sharing Overview

Load sharing is to forward data traffic through multiple activated links existing between equipment and to fully take use of the bandwidth of multiple links. Load sharing does not mean that data traffic on links have same size.

Data traffic covers incoming and outgoing traffic. Incoming and outgoing traffic load sharing is closely related to the route announced outside and learned by the equipment. Incoming traffic load sharing is affected by internal route announced outside by the equipment and outgoing traffic load sharing is affected by route announced inside by the equipment. They directly affect the installation of multiple route entries reaching the destination in the equipment forwarding table and the control of multiple routes.

ZXR10 8900 series switch adopts route-based load sharing to install multiple reachable route entries for a destination address in the forwarding table through configuring static route, routing protocol and number of hops, thus laying foundation for load sharing implementation.

ZXR10 8900 series switch supports per-destination load sharing policy. This policy considers source addresses and destination addresses of packets at the same time and make the packets with same "source address-destination address" pair pass through the same path (even there are multiple available paths), and the packets with different "source address-destination address" pairs pass through different paths. Such a policy ensures the packets with the same "source address-destination address" pair to arrive in order. Load sharing becomes more effective if there are multiple "source address-destination address" pairs in traffic.

Eight different paths can arrive at the destination at most on ZXR10 8900 series switch. Once load sharing is configured, interface traffic becomes balanced after a period.

Configuring Load Sharing

To configure load sharing, perform the following steps.

Step	Command	Function
1	<code>ZXR10(config-router)#maximum-paths <number></code>	This configures maximum number of paths allowed in load sharing.
2	<code>ZXR10(config)#ip route [vrf <vrf-name>]<prefix><net-mask>{<forwarding-router's-address> <interface-name>}[<distance-metric>][tag <tag>]</code>	This configures load sharing through static route.



Note:

For step 1, maximum number of paths can be configured in RIP, OSPF, IS-IS and BGP routing configuration modes. Default number of paths is 1. Up to 8 paths are supported.

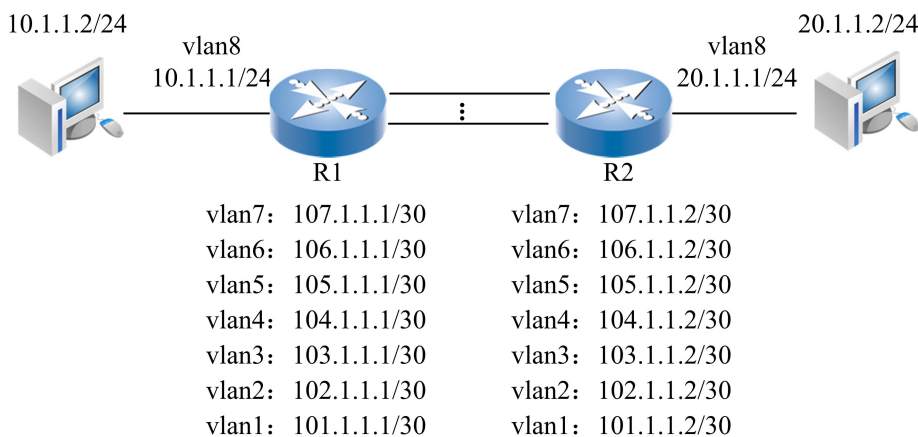
For step 2, number of multiple static routes to one destination is up to 8 on a device. These routes should have different tags.

Load Sharing Configuration Examples

Load Sharing through Static Route

R1 is connected to R2 over seven links. This is shown in [Figure 25](#).

FIGURE 25 LOAD SHARING CONFIGURATION EXAMPLE



To configure load sharing through static route, the configuration is shown below.

Configuration on R1:

```
ZXR10_R1(config)#interface vlan1
ZXR10_R1(config-if)#ip address 101.1.1.1 255.255.255.252
ZXR10_R1(config)#interface vlan2
ZXR10_R1(config-if)#ip address 102.1.1.1 255.255.255.252
ZXR10_R1(config)#interface vlan3
ZXR10_R1(config-if)#ip address 103.1.1.1 255.255.255.252
ZXR10_R1(config)#interface vlan4
ZXR10_R1(config-if)#ip address 104.1.1.1 255.255.255.252
ZXR10_R1(config)#interface vlan5
ZXR10_R1(config-if)#ip address 105.1.1.1 255.255.255.252
ZXR10_R1(config)#interface vlan6
ZXR10_R1(config-if)#ip address 106.1.1.1 255.255.255.252
ZXR10_R1(config)#interface vlan7
ZXR10_R1(config-if)#ip address 107.1.1.1 255.255.255.252
ZXR10_R1(config)#interface vlan8
ZXR10_R1(config-if)#ip address 10.1.1.1 255.255.255.0

ZXR10_R1(config)#ip route 20.1.1.0 255.255.255.0
107.1.1.2 1 tag 157
ZXR10_R1(config)#ip route 20.1.1.0 255.255.255.0
106.1.1.2 1 tag 156
ZXR10_R1(config)#ip route 20.1.1.0 255.255.255.0
105.1.1.2 1 tag 155
ZXR10_R1(config)#ip route 20.1.1.0 255.255.255.0
104.1.1.2 1 tag 154
ZXR10_R1(config)#ip route 20.1.1.0 255.255.255.0
103.1.1.2 1 tag 153
ZXR10_R1(config)#ip route 20.1.1.0 255.255.255.0
102.1.1.2 1 tag 152
ZXR10_R1(config)#ip route 20.1.1.0 255.255.255.0
101.1.1.2 1 tag 151
```

Configuration on R2:

```
ZXR10_R2(config)#interface vlan1
ZXR10_R2(config-if)#ip address 101.1.1.2 255.255.255.252
ZXR10_R2(config)#interface vlan2
ZXR10_R2(config-if)#ip address 102.1.1.2 255.255.255.252
ZXR10_R2(config)#interface vlan3
ZXR10_R2(config-if)#ip address 103.1.1.2 255.255.255.252
ZXR10_R2(config)#interface vlan4
ZXR10_R2(config-if)#ip address 104.1.1.2 255.255.255.252
ZXR10_R2(config)#interface vlan5
ZXR10_R2(config-if)#ip address 105.1.1.2 255.255.255.252
ZXR10_R2(config)#interface vlan6
ZXR10_R2(config-if)#ip address 106.1.1.2 255.255.255.252
ZXR10_R2(config)#interface vlan7
ZXR10_R2(config-if)#ip address 107.1.1.3 255.255.255.252
ZXR10_R2(config)#interface vlan8
ZXR10_R2(config-if)#ip address 20.1.1.1 255.255.255.0

ZXR10_R2(config)#ip route 10.1.1.0 255.255.255.0
107.1.1.1 1 tag 157
ZXR10_R2(config)#ip route 10.1.1.0 255.255.255.0
106.1.1.1 1 tag 156
ZXR10_R2(config)#ip route 10.1.1.0 255.255.255.0
105.1.1.1 1 tag 155
ZXR10_R2(config)#ip route 10.1.1.0 255.255.255.0
104.1.1.1 1 tag 154
ZXR10_R2(config)#ip route 10.1.1.0 255.255.255.0
103.1.1.1 1 tag 153
ZXR10_R2(config)#ip route 10.1.1.0 255.255.255.0
102.1.1.1 1 tag 152
ZXR10_R2(config)#ip route 10.1.1.0 255.255.255.0
101.1.1.1 1 tag 151
```

Seven links between R1 and R2 implement load sharing and over these links, the user PC1 and the user PC2 can access each other.

Load Sharing through OSPF

For the topology shown in the above example, configuration of load sharing through OSPF is shown below.

Configuration on R1:

```
ZXR10_R1(config)#router ospf 100
ZXR10_R1(config-router)#network 101.1.1.0 0.0.0.3 area 0.0.0.0
ZXR10_R1(config-router)#network 102.1.1.0 0.0.0.3 area 0.0.0.0
ZXR10_R1(config-router)#network 103.1.1.0 0.0.0.3 area 0.0.0.0
ZXR10_R1(config-router)#network 104.1.1.0 0.0.0.3 area 0.0.0.0
ZXR10_R1(config-router)#network 105.1.1.0 0.0.0.3 area 0.0.0.0
ZXR10_R1(config-router)#network 106.1.1.0 0.0.0.3 area 0.0.0.0
ZXR10_R1(config-router)#network 107.1.1.0 0.0.0.3 area 0.0.0.0
ZXR10_R1(config-router)#network 10.1.1.0 0.0.0.255 area 0.0.0.0
ZXR10_R1(config-router)#maximum-paths 7
```

Configuration on R2:

```
ZXR10_R2(config)#router ospf 100
ZXR10_R2(config-router)#network 101.1.1.0 0.0.0.3 area 0.0.0.0
ZXR10_R2(config-router)#network 102.1.1.0 0.0.0.3 area 0.0.0.0
ZXR10_R2(config-router)#network 103.1.1.0 0.0.0.3 area 0.0.0.0
ZXR10_R2(config-router)#network 104.1.1.0 0.0.0.3 area 0.0.0.0
ZXR10_R2(config-router)#network 105.1.1.0 0.0.0.3 area 0.0.0.0
ZXR10_R2(config-router)#network 106.1.1.0 0.0.0.3 area 0.0.0.0
ZXR10_R2(config-router)#network 107.1.1.0 0.0.0.3 area 0.0.0.0
ZXR10_R2(config-router)#network 20.1.1.0 0.0.0.255 area 0.0.0.0
ZXR10_R2(config-router)#maximum-paths 7
```

Load Sharing Maintenance and Diagnosis

To configure load sharing maintenance and diagnosis, use the following command.

Command	Function
ZXR10# show ip route [<i><ip-address></i>][<i><net-mask></i>][<i><protocol></i>]	This displays load sharing configuration and running information.

Example This example describes seven paths reaching destination network segment 20.1.1.0/24 on R1 when adopting static route load sharing.

```
ZXR10_R1#show ip route 20.1.1.0
IPv4 Routing Table:
  Dest      Mask      Gw      Interface  Owner  pri  metr
20.1.1.0    255.255.255.0  107.1.1.1  vlan7      static  1    0
20.1.1.0    255.255.255.0  106.1.1.1  vlan6      static  1    0
20.1.1.0    255.255.255.0  105.1.1.1  vlan5      static  1    0
20.1.1.0    255.255.255.0  104.1.1.1  vlan4      static  1    0
20.1.1.0    255.255.255.0  103.1.1.1  vlan3      static  1    0
20.1.1.0    255.255.255.0  102.1.1.1  vlan2      static  1    0
20.1.1.0    255.255.255.0  101.1.1.1  vlan1      static  1    0
```

It can be seen that seven paths reaching the destination network segment 20.1.1.0/24 on R1 when adopting dynamic route protocol OSPF load sharing.

```
ZXR10_R1#show ip route 20.1.1.0
```

```
IPv4 Routing Table:
```

Dest	Mask	Gw	Interface	Owner	pri	metr
20.1.1.0	255.255.255.0	107.1.1.1	vlan7	ospf	110	2
20.1.1.0	255.255.255.0	106.1.1.1	vlan6	ospf	110	2
20.1.1.0	255.255.255.0	105.1.1.1	vlan5	ospf	110	2
20.1.1.0	255.255.255.0	104.1.1.1	vlan4	ospf	110	2
20.1.1.0	255.255.255.0	103.1.1.1	vlan3	ospf	110	2
20.1.1.0	255.255.255.0	102.1.1.1	vlan2	ospf	110	2
20.1.1.0	255.255.255.0	101.1.1.1	vlan1	ospf	110	2

This page is intentionally blank.

Multicast Route Configuration

Table of Contents

IP Multicast Overview	71
Enabling IP Multicast.....	75
Enabling IP Multicast Load Sharing.....	75
Configuring IGMP	76
Configuring Static IP Multicast.....	78
Configuring PIM-SM	79
Configuring MSDP.....	85
IP Multicast Configuration Example	88
IP Multicast Maintenance and Diagnosis.....	90

IP Multicast Overview

IP multicast is a point-to-multipoint or multipoint-to-multipoint communication. That is, multiple receivers receive the same information from one source at the same time. IP multicast based applications include video-conferencing, distance learning and software distribution.

IP multicast protocols include Internet Group Management Protocol (**IGMP**) and Multicast Route Protocols (MRP). IGMP is used to manage participation and leaving of multicast group members. MRPs are used to exchange information and establish multicast tree among routers. MRPs include Protocol Independent Multicast Sparse Mode (**PIM-SM**) and Multicast Source Discovery Protocol (**MSDP**).

ZXR10 8900 series switch supports the following protocols:

- Internet Group Management Protocol (IGMP)
- Protocol Independent Multicast Sparse Mode (PIM-SM)
- Multicast Source Discovery Protocol (MSDP)

IP Multicast Address

In an IP multicast network, the originator sends a packet to multi receivers by IP multicast. The originator is called mul-

ticast source. The multiple receivers of the same packet are identified by using a single ID, which is called multicast group address. In IP address allocation scenario, addresses of Class-D (224.0.0.0~239.255.255.255) are multicast group addresses. 224.0.0.0~224.0.0.255 and 239.0.0.0~239.255.255.255 are used for research and management.

IGMP

IGMP allows multicast router to learn information of multicast group members. IGMP runs between host and multicast router.

A multicast router sends group member query messages to all hosts periodically to learn which group members exist in the connected networks. Each host returns a group member report message. The message contains multicast group information and it reports which group the host belongs to. When a host wants to be added to a new group, it sends a group member report message immediately instead of waiting for a query.

When a host begins to receive information as a group member, the multicast router queries the group periodically to learn whether this member is still in the group. If members of the group still exist on an interface, the multicast router continues to forward data. When the host leaves the group, it sends a leaving message to the multicast router. The multicast router immediately queries whether the group still contains active members or not. If yes, the multicast router continues to forward data; if no, it stops forwarding data.

There are two versions of IGMP in practical applications, IGMP V1 and IGMP V2. IGMP V2 has more enhanced features than IGMP V1. It uses 4 types of messages to accomplish information interaction between hosts and router.

- Group member query
- V2 member report
- Leave report
- V1 member report

V1 member report is used to be compatible with IGMP V1.

Multicast Tree

To enable multicast communication in the networks, the multicast source, receivers and the paths of multicast packets should be available. The most commonly used routing method is to establish tree routes, which provides the following two advantages:

- Packets are sent to different receivers along the tree branches in parallel.
- Packets are copied only on crotches, which minimizes the number of packets transmitted in the networks.

A multicast tree is a set that comprises a series of incoming interfaces and outgoing interfaces on router. It determines a unique forwarding path between the subnet to which the multicast source belongs and all the subnets that contain the group members.

There are two ways to construct a multicast tree: per-source multicast tree and shared multicast tree.

Per-Source Multicast Tree

Per-source multicast tree is also called source shortest path tree. It establishes a spanning tree to all receivers for each source. This spanning tree takes the subnet to which the source belongs as the root node. This tree reaches the subnets to which the receivers belong. A multicast group may include multi multicast sources. Each source or pair (S, G) has a corresponding multicast tree.

The method to construct a per-source multicast tree is reverse path forwarding (RPF). Each router can find the shortest path to the source and the corresponding outgoing interface according to uni-cast route. When a router receives a multicast packet, it verifies whether the incoming interface that the packet reaches is the outgoing interface to the source with the shortest uni-cast path. If yes, the route copies the packet and forwards it to outgoing interfaces; otherwise, it discards the multicast packet.

The incoming interface from which the router receives multicast packets is called parent link. The outgoing interface that sends multicast packets is called child link.

Shared Multicast Tree

Shared multicast tree establishes a multicast route tree for each multicast group, which is shared by all group members. That is, the tree is shared by the group (*, G) instead of every pair (S, G). Each device to receive the multicast packets from the group should be added to the shared tree explicitly.

A shared multicast tree uses one or a group of routers as the center of the tree. Multicast packets from all sources in this group to the receivers are sent as uni-cast packets to the center. Then these packets are forwarded as multicast packets along the tree from the center.

PIM-SM

PIM-SM uses a shared tree to transmit multicast packets. A shared tree has a central point, which is responsible for sending packets for all the sources in a multicast group. Each source sends packets to the central point along the shortest-path route. Then the source takes the central point as root node to distribute the packets to all the receivers in the group. The central point of a PIM-SM group is called Rendezvous Point (RP). A network is allowed to have multiple RPs, but a multicast group only has one RP.

A router can obtain the location of the RP by three methods.

- Configure RPs manually and statically on various routers running the PIM-SM.
- PIM-SM V1 obtains such locations through automatic RPs dynamically.

- PIM-SM V2 obtains such locations through the candidate-RP notification. The candidate-RPs with higher priority will become formal RPs.

PIM-SM V2 manually configures some routers running PIM-SM as candidate-BSRs (BootStrap Router), and selects the candidate-BSR with the highest priority as the formal BSR. BSR is responsible for collecting candidate RP messages from the entire multicast routers. It also tries to find the candidate RPs existing in the multicast domain and advertises them to all the PIM routers in the PIM domain. Each PIM router selects the optimum RP for each group in the RP set according to the unified RP election rule. RP candidates are configured manually.

Routers running PIM-SM attempt to find each other and maintain the neighbor relation by exchanging hello messages. On the multi-access network, a hello message also includes router priority information. It is used to elect the designated router (DR).

Multicast source or the first-hop router (DR directly connected to the source) encapsulates the packet into a Register message and sends it to RP through a uni-cast route. When receiving the Register message, RP de-encapsulates the packet and sends it along the shared tree downward to receivers in this group.

Each host acting as a receiver joins multicast group by an IGMP member report message. The last-hop router (or DR on the multi-access network) sends received Join message to RP level by level for registration. The media router checks if a route for this group is available after receiving Join message. If yes, it adds the downstream requesting router to the shared tree as a branch. Otherwise, it creates a route for the group with the incoming interface pointing to the RP and the outgoing interface pointing to the downstream requesting router, and then the Join message proceeds to RP continuously level by level.

When the RP or multicast router is directly connected to any receiver, it can be switched over from the shared tree to the per-source multicast tree. When receiving a Register message from a new multicast source, RP returns a Join message to DR that is directly connected to multicast source. Thus, the shortest path tree from the source to the RP is established.

When a DR or a router with multicast members connected directly receives the first multicast packet from the multicast group, or when the received packets reach a threshold, it can be switched over from the shared tree to the per-source, shortest-path tree. Once the switchover occurs, the route will send a Prune message to the upstream neighbors, requesting to be separated from the shared tree.

MSDP

MSDP is a mechanism that allows RPs in each PIM-SM domain to share information about active sources. Each RP knows the receivers within the local domain. When RPs has learned information about active sources in remote domains, they can transfer the information to receivers in local domain. Thus, multicast packets can be forwarded among domains.

MSDP speaker in a PIM-SM domain establishes MSDP peering session with MSDP peers in other domains through TCP connection. When MSDP speaker has learnt a new multicast source (through the PIM register mechanism) in local domain, it creates a Source-Active message and sends it to all the MSDP peers.

Each MSDP peer that receives the message uses peer-RPF check and only the SA message received on correct interface is forwarded, discarding the others. When an MSDP peer which is also an RP for its own domain receives a new SA message and the outgoing interface list in (*, G) entry is non-empty, that is, there are receivers within the domain, RP creates a (S, G) state for multicast source and adds this entry to the shortest-path tree of the source.

In addition, each MSDP peer saves the received SA messages in a cache, thus establishing a SA cache table. If the RP in a PIM-SM domain receives a new PIM join message for multicast group G, the RP searches its own SA cache table to get all the active multicast sources immediately, thus generating the corresponding (S, G) Join message.

Enabling IP Multicast

To enable IP multicast, use the following command.

Command	Function
ZXR10 (config) # ip multicast-routing	This enables IP multicast



Note:

To disable IP multicast, use **no ip multicast-routing** command.

Enabling IP Multicast Load Sharing

Command	Function
ZXR10 (config) # ip multicast-loading	This enables IP multicast load sharing function.

To disable IP multicast load sharing function, execute command **no ip multicast-loading**.

Configuring IGMP

Configuring IGMP Version

IGMP versions include V1 and V2. Default value is V2, which can be changed according to requirement. In view of security requirements, the routes require all the network elements in the same network to use IGMP V1 or IGMP V2 simultaneously.

Configuration of IGMP version is based on interface. Different interfaces can be configured with different versions.

To configure IGMP version on interface, perform the following steps.

Step	Command	Function
1	ZXR10(config)# interface vlan <vlan-id>	This enters interface configuration mode
2	ZXR10(config-if)# ip igmp version <version>	This configures IGMP version on interface

Configuring IGMP Group on Interface

To configure IGMP group on interface, perform the following steps.

Step	Command	Function
1	ZXR10(config-if)# ip igmp access-group <access-list-number>	This configures the range of groups to which IGMP is allowed to be added
2	ZXR10(config-if)# ip igmp immediate-leave [group-list <access-list-number>]	This configures the range of groups from which IGMP is allowed to leave immediately
3	ZXR10(config-if)# ip igmp static-group <group-address>	This configures static group members on an IGMP interface



Note:

For step 1, when IGMP is running on an interface, all multicast groups are received by default. The range of receiving groups can be set. If the Join request from a host does not belong to the range, it is discarded.

For step 2, after receiving an IGMP Leave message or if no report message is received after (last member query interval×2+1) seconds, group members will leave.

For step 3, static group address can be bound on an interface, suppose there always are group members on this interface.

Example This example shows how to configure to receive group 239.10.10.10 only on interface vlan1.

```
ZXR10(config)#acl standard number 10
ZXR10(config-std-acl)#rule 1 permit 239.10.10.10 0.0.0.0
ZXR10(config)#interface vlan 1
ZXR10(config-if)#ip igmp access-group 10
```

Example This example shows how to allow group 239.10.10.10 to leave immediately from interface vlan1.

```
ZXR10(config)#acl basic number 10
ZXR10(config-basic-acl)#rule 1 permit 239.10.10.10 0.0.0.0
ZXR10(config)#interface vlan 1
ZXR10(config-if)#ip igmp immediate-leave group-list 10
```

Example This example shows how to configure static group 239.10.10.10 on interface vlan1.

```
ZXR10(config)#interface vlan 1
ZXR10(config-if)#ip igmp static-group 239.10.10.10
```

Configuring IGMP Timers

After enabling IGMP on multicast router interfaces that is connected to the shared network, the optimum router is elected as the query router in this network. Query router is responsible for obtaining group member information by sending query messages.

After sending a query message, query router waits for receiving Host Membership Reports in a period of time. The duration is the value of max response time contained in the query message sent, 10 seconds by default. After receiving query message, host members in the network take the result of max response time minus a random offset value as their own response time. If other Host Member Reports are received in this period, it is cancelled, otherwise, host reports are sent at the response time. Therefore, increasing the max response time extends the waiting time of group members and lowers occurrence of multi host reports in the network.

To configure IGMP timers, perform the following steps.

Step	Command	Function
1	ZXR10(config-if)# ip igmp query-interval <seconds>	This configures IGMP query interval
2	ZXR10(config-if)# ip igmp querier-timeout <seconds>	This configures IGMP query router timeout

Step	Command	Function
3	ZXR10(config-if)# ip igmp query-max-response-time <seconds>	This configures the max response time contained in the query message sent by IGMP
4	ZXR10(config-if)# ip igmp last-member-query-interval <seconds>	This configures IGMP specific group query interval

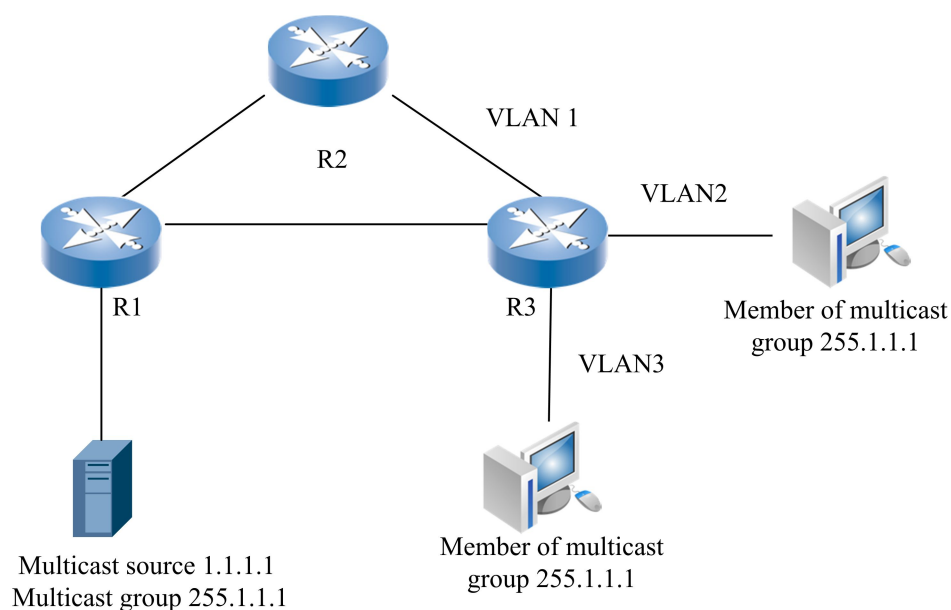
Configuring Static IP Multicast

To configure static IP multicast, perform the following steps.

Step	Command	Function
1	ZXR10(config)# ip multicast-routing	This enables IP multicast
2	ZXR10(config)# ip multicast-static-start	This enables static IP multicast
3	ZXR10(config)# p multicast-static-interface index <index-number> vlan <1-4094>	This configures the VLAN to receive multicast group
4	ZXR10(config)# ip multicast-static-limit xg <1-1024> sg <1-1024>	This limits the number of IP multicast route items. xg means (*,g) and sg means (s,g)
5	ZXR10(config)# ip multicast-static-route <source><group>[iif <interfacename>][oif <index-number>]	This configures static IP multicast route

Example As shown in [Figure 26](#), R1 connects with a multicast source 1.1.1.1 and R3 connects with two group members.

FIGURE 26 STATIC IP MULTICAST CONFIGURATION EXAMPLE



Configuration on R3:

```
ZXR10(config)#ip multicast-routing
ZXR10(config)#ip multicast-static-start
ZXR10(config)#ip multicast-static-interface index 1 vlan 2-3
ZXR10(config)#ip multicast-static-limit xg 16 sg 16
ZXR10(config)#ip multicast-static-route 1.1.1.1
225.1.1.1 iif vlan1 oif 1
```

Use the same method to configure R1 and R2.

Configuring PIM-SM

Enabling PIM-SM

To enable PIM-SM, perform the following steps.

Step	Command	Function
1	<code>ZXR10(config)#router pimsm</code>	This enables PIM-SM process globally
2	<code>ZXR10(config)#interface <interface-name></code>	This enters interface configuration mode
3	<code>ZXR10(config-if)#ip pim sm</code>	This adds an interface that runs PIM-SM

Configuring Static RP

A static RP can be configured for one or more specific groups, and the same static RP should be configured for the group on all PIM-SM multicast routers in the multicast domain. RP addresses should be reachable from other routers. Use loopback interface address to reduce the network oscillations due to physical interface up/down. When a static RP is configured, the candidate RP is not needed for the group.

To configure static RP, perform the following steps.

Step	Command	Function
1	ZXR10(config)# router pimsm	This enters PIM-SM configuration mode
2	ZXR10(config-router)# static-rp <ip-address>[group-list <access-list-number>][priority <priority>]	This configures static RP

Example This example shows how to configure static RP 10.1.1.1 for all groups.

```
ZXR10(config-router)#static-rp 10.1.1.1
```

This example shows how to configure static RP 10.1.1.1 for group 239.132.10.100.

```
ZXR10(config-router)#static-rp 10.1.1.1 group-list 10
ZXR10(config)#acl basic number 10
ZXR10(config-basic-acl)#rule 1 permit 239.132.10.100 0.0.0.0
```

Configuring Candidate BSR

When static RP mechanism is not used, candidate BSRs should be configured on one or more than one multicast routers in each multicast domain. The BSR sends bootstrap (BSR) messages periodically to advertise RP conditions. Routers running PIM-SM update the RP states according to the latest advertisement messages. The bootstrap messages sent by BSR are also used to elect formal BSR from the candidate BSRs.

To configure candidate BSR, perform the following steps.

Step	Command	Function
1	ZXR10(config)# router pimsm	This enters PIM-SM configuration mode
2	ZXR10(config-router)# bsr-candidate <interface-name>[<hash-mask-length>][<priority>]	This configures candidate BSR

**Note:**

Default priority of a candidate BSR is 0. Candidate BSR with the highest priority becomes the formal BSR. If multiple routers have the same BSR priority, IP addresses are compared. Candidate BSR with the largest address becomes the formal BSR.

Configuring Candidate RP

In PIM-SM, RP is the root of a shared multicast tree. It is responsible for sending multicast packets to the downstream receiving group members along the shared tree. A multicast group can only have one formal RP.

To configure candidate RP, perform the following steps.

Step	Command	Function
1	ZXR10 (config) # router pimsm	This enters PIM-SM configuration mode
2	ZXR10 (config-router) # rp-candidate <interface-name> [group-list <access-list-number>] [priority <priority>]	This configures candidate RP

**Note:**

The default priority of a candidate RP is 192. The candidate RP with a bigger priority is preferred.

Applying Static RP for the same RP Priorities

There can be only one formal RP in each one multicast group. RP is elected according to priorities. When both static rp and dynamic rp are available and both have the same priority, formal rp will be elected according to their IP addresses.

Step	Command	Function
1	ZXR10 (config) # router pimsm	This enters PIM-SM configuration mode.
2	ZXR10 (config-router) # static-rp override	This configures static rp override function.

Switching over to Source Shortest Path Tree

Only the last-hop DR and RP can switch over to the source shortest path tree. By default, switchover begins when RP has received the first Register message. For the last-hop DR, the switchover threshold policy can be configured with single uni-cast group as the granularity of control. If the shortest path tree threshold is configured as infinite, no switchover occurs. By default, a switchover will occur if only there is flow.

To switch over to source shortest path tree, perform the following steps.

Step	Command	Function
1	<code>ZXR10(config)#router pimsm</code>	This enters PIM-SM configuration mode
2	<code>ZXR10(config-router)#spt-threshold infinity</code> <code>[group-list <access-list-number>]</code>	This configures the router that is connected to receivers directly to switch over from shortest path tree back to shared tree (RP tree)

Filtering Received Register Messages

Source addresses in multicast data messages encapsulated in the Register messages are filtered according to the rules defined in the ACL.

To filter received register messages on RP, perform the following steps.

Step	Command	Function
1	<code>ZXR10(config)#router pimsm</code>	This enters PIM-SM configuration mode
2	<code>ZXR10(config-router)#accept-register <access-list-number></code>	This filters received register messages on RP

Filtering Candidate RP

To filter candidate RPs that are advertised by BSR messages, perform the following steps.

Step	Command	Function
1	ZXR10 (config) # router pimsm	This enters PIM-SM configuration mode
2	ZXR10 (config-router) # accept-rp <access-list-number>	This filters candidate RPs that are advertised by BSR messages

Configuring PIM Domain Border

To configure an interface as the PIM domain border, perform the following steps.

Step	Command	Function
1	ZXR10 (config) # interface vlan<vlan-id>	This enters interface configuration mode
2	ZXR10 (config-if) # ip pim bsr-border	This configures an interface as the PIM domain border



Note:

When this command is configured on an interface, bootstrap data messages are not able to pass through the border in any direction. This command allows a network to be divided into areas using different BSRs. However, other PIM messages can pass through the domain border.

Configuring DR Priority

A DR should be elected from a shared (or multi-access) network. The router with the highest priority is elected. If the routers have the same priority, the one with the largest IP address is selected.

In the shared network segment that is connected to the multi-cast data source, only DR can send Register messages to RP. In the shared network segment that is connected to the receivers, only DR can respond to IGMP Join/Leave messages and send PIM Join/Prune messages to upstream routers.

To configure DR priority, perform the following steps.

Step	Command	Function
1	ZXR10 (config) # interface vlan<vlan-id>	This enters interface configuration mode
2	ZXR10 (config-if) # ip pim dr-priority <priority>	This configures DR priority

Ignoring DR Election

DR election is necessary on a shared network. When a DR is the first hop, it implements source registration. When a DR is the last hop, that is, the receiver, it implements joining of multicast group. After normal DR election, non-DRs can not reply requirements of IGMP join or IGMP leave.

If DR election is ignored, each device is a DR. They can reply requirements of IGMP join or IGMP leave from the downlink users and send joining messages or pruning messages to upstream devices. By default, DR election is enabled.

To ignore DR election, perform the following steps.

Step	Command	Function
1	ZXR10(config)# interface vlan <vlan-id>	This enters interface configuration mode
2	ZXR10(config-if)# ip pim ignore-dr	This ignores DR election

Configuring SM/DM Hybrid Mode

To configure SM/DM hybrid mode, perform the following steps.

Step	Command	Function
1	ZXR10(config)# interface vlan <vlan-id>	This enters interface configuration mode
2	ZXR10(config-if)# ip pim smdm-hybrid	This enables SM/DM hybrid mode function



Note:

After SM/DM hybrid mode function is enabled on an interface, multicast traffic flows to PIM neighbor interface of a VLAN interface without any condition.

SM/DM hybrid mode function is effective only when both PIM SM and PIM SNOOPING are configured.

By default, M/DM hybrid mode function is disabled.

Configuring Hello Message Interval

To set hello message interval, perform the following steps.

Step	Command	Function
1	ZXR10 (config) # interface vlan <vlan-id>	This enters interface configuration mode
2	ZXR10 (config-if) # ip pim query-interval <seconds>	This configures hello message interval

**Note:**

The interval of hello messages sent by PIM-SM neighbors can be adjusted according to the network conditions. By default, it is 30 seconds.

Limiting PIM-SM Neighbors

According to security requirements, PIM-SM can refuse some of the routers to be neighbors on an interface.

To limit PIM-SM neighbors, perform the following steps.

Step	Command	Function
1	ZXR10 (config) # interface vlan <vlan-id>	This enters interface configuration mode
2	ZXR10 (config-if) # ip pim neighbor-filter <access-list-number>	This limits PIM-SM neighbors

Example This example shows how to limit PIM-SM neighbors.

Router 10.1.1.1 is not allowed to be a PIM neighbor on interface vlan1.

```
ZXR10(config)#acl basic number 10
ZXR10(config-basic-acl)#rule 1 deny 10.1.1.1 0.0.0.0
ZXR10(config-basic-acl)#rule 2 permit any
ZXR10(config)#interface vlan 1
ZXR10(config-if)#ip pim neighbor-filter 10
```

Configuring MSDP

Enabling MSDP

To configure an MSDP peer and enable MSDP, use the following command.

Command	Function
<code>ZXR10(config)#ip msdp peer <peer-address> connect-source <interface-name></code>	This configures an MSDP peer and enables MSDP

Configuring Default MSDP Peer

To configure default MSDP peer, use the following command.

Command	Function
<code>ZXR10(config)#ip msdp default-peer <peer-address>[list <acl-number>]</code>	This configures default MSDP peer



Note:

When default MSDP peer is configured, the local router accepts all SA messages from the peer.

Configuring Originating RP

To configure an originating RP, use the following command.

Command	Function
<code>ZXR10(config)#ip msdp originator-id <interface-name></code>	This configures an originating RP



Note:

This command generates the MSDP speaker of SA messages. It also uses address of specified interface as the RP address in a SA.

Configuring MSDP Peer as Mesh Group Member

A mesh group is a group of MSDP speakers. These speakers have fully meshed connectivity.

To configure the MSDP peer as a mesh group member, use the following command.

Command	Function
ZXR10 (config) # ip msdp mesh-group <peer-address><mesh-name>	This configures the MSDP peer as a mesh group member

Limiting the Number of SA Messages

To configure the maximum number of SA messages allowed in the SA cache, use the following command.

Command	Function
ZXR10 (config) # ip msdp sa-limit <peer-address><sa-limit>	This configures the maximum number of SA messages allowed in the SA cache

Shutting Down Peers Configured MSDP

To shut down peers that are configured MSDP, use the following command.

Command	Function
ZXR10 (config) # ip msdp shutdown <peer-address>	This shuts down peers that are configured MSDP

Clearing TCP Connection

To clear TCP connections established with MSDP peers, use the following command.

Command	Function
ZXR10# clear ip msdp peer [<peer-address>]	This clears TCP connections established with MSDP peers

**Note:**

This command shuts down TCP connections to MSDP peers and resets all statistics of MSDP peers.

Clearing Entries in MSDP SA Cache

To clear entries in MSDP SA cache, use the following command.

Command	Function
zxr10# clear ip msdp sa-cache [<group-address>]	This clears entries in MSDP SA cache

Clearing Statistics Counter for MSDP Peers

To clear statistics counter for MSDP peers, use the following command.

Command	Function
zxr10# clear ip msdp statistics [<peer-address>]	This clears statistics counter for MSDP peers

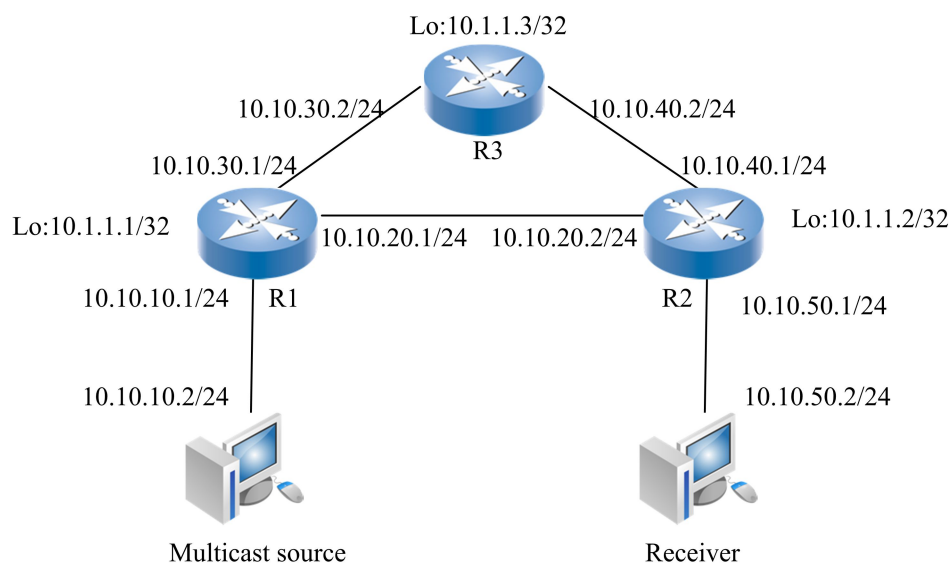
**Note:**

This command clears the statistics counter for the MSDP peer but does not reset the MSDP sessions.

IP Multicast Configuration Example

This example shows PIM-SM configuration. Network topology is shown in [Figure 27](#).

FIGURE 27 IP MULTICAST CONFIGURATION EXAMPLE



Configuration on R1:

```
ZXR10_R1(config)#interface loopback1
ZXR10_R1(config-if)#ip address 10.1.1.1 255.255.255.255
ZXR10_R1(config-if)#exit
ZXR10_R1(config)#ip multicast-routing
ZXR10_R1(config)#router pimsm
ZXR10_R1(config-router)#rp-candidate loopback1 priority 10
ZXR10_R1(config-router)#bsr-candidate loopback1 10 10
ZXR10_R1(config-router)#exit
ZXR10_R1(config)#interface vlan1
ZXR10_R1(config-if)#ip address 10.10.10.1 255.255.255.0
ZXR10_R1(config-if)#ip pim sm
ZXR10_R1(config-if)#exit
ZXR10_R1(config)#interface vlan2
ZXR10_R1(config-if)#ip address 10.10.20.1 255.255.255.0
ZXR10_R1(config-if)#ip pim sm
ZXR10_R1(config-if)#exit
ZXR10_R1(config)#interface vlan3
ZXR10_R1(config-if)#ip address 10.10.30.1 255.255.255.0
ZXR10_R1(config-if)#ip pim sm
ZXR10_R1(config-if)#exit
ZXR10_R1(config)#router ospf 1
ZXR10_R1(config-router)#network 10.0.0.0 0.0.0.255 area 0.0.0.0
```

Configuration on R2:

```
ZXR10_R2(config)#interface loopback1
ZXR10_R2(config-if)#ip address 10.1.1.2 255.255.255.255
ZXR10_R2(config-if)#exit
ZXR10_R2(config)#ip multicast-routing
ZXR10_R2(config)#router pimsm
ZXR10_R2(config-router)#rp-candidate loopback1 priority 20
ZXR10_R2(config-router)#bsr-candidate loopback1 10 20
ZXR10_R2(config-router)#exit
ZXR10_R2(config)#interface vlan1
ZXR10_R2(config-if)#ip address 10.10.20.2 255.255.255.0
ZXR10_R2(config-if)#ip pim sm
ZXR10_R2(config-if)#exit
ZXR10_R2(config)#interface vlan2
ZXR10_R2(config-if)#ip address 10.10.40.1 255.255.255.0
ZXR10_R2(config-if)#ip pim sm
ZXR10_R2(config-if)#exit
ZXR10_R2(config)#interface vlan3
ZXR10_R2(config-if)#ip address 10.10.50.1 255.255.255.0
ZXR10_R2(config-if)#ip igmp access-group 10
ZXR10_R2(config-if)#exit
```

```
ZXR10_R2(config)#router ospf 1
ZXR10_R2(config-router)#network 10.0.0.0 0.0.0.255 area 0.0.0.0
ZXR10_R2(config-router)#exit
ZXR10_R2(config)#access-list 10 permit any
```

Configuration on R3:

```
ZXR10_R3(config)#interface loopback1
ZXR10_R3(config-if)#ip address 10.1.1.3 255.255.255.255
ZXR10_R3(config-if)#exit
ZXR10_R3(config)#ip multicast-routing
ZXR10_R3(config)#router pimsm
ZXR10_R3(config-router)#rp-candidate loopback1 priority 30
ZXR10_R3(config-router)#bsr-candidate loopback1 10 30
ZXR10_R3(config-router)#exit
ZXR10_R3(config)#interface vlan1
ZXR10_R3(config-if)#ip address 10.10.30.2 255.255.255.0
ZXR10_R3(config-if)#ip pim sm
ZXR10_R3(config-if)#exit
ZXR10_R3(config)#interface vlan2
ZXR10_R3(config-if)#ip address 10.10.40.2 255.255.255.0
ZXR10_R3(config-if)#ip pim sm
ZXR10_R3(config-if)#exit
ZXR10_R3(config)#router ospf 1
ZXR10_R3(config-router)#network 10.0.0.0 0.0.0.255 area 0.0.0.0
```



Note:

Pay attention to the sequence of configuration. The **ip multicast-routing** is configured prior to **router pimsm**. Next, enable **ip pim sm** on the interface. The configuration will not be successful if the sequence is not followed.

IP Multicast Maintenance and Diagnosis

ZXR10 8900 series switch supports maintenance and diagnosis commands for different multicast protocols.

Public IP Multicast Maintenance and Diagnosis

To configure public IP multicast maintenance and diagnosis, perform the following steps.

Step	Command	Function
1	<code>ZXR10#show ip mroute [group <group-address>][source <source-address>][summary brief]</code>	This displays IP multicast routing table
2	<code>ZXR10#show ip mforwarding module <number>{summary {group-address <group-address>[source-address <source-address>]}}</code>	This displays multicast forwarding route entries

Step	Command	Function
3	ZXR10# show ip rpf <source-address>	This displays information of multicast RPF
4	ZXR10# clear ip mroute [group-address <group-address>][source-address <source-address>]]	This deletes multicast routing table

**Note:**

For command in step 2, when this command does not contain any source address option, it displays the (*, G) and (S, G) multicast forwarding entries. If it contains a source address option, it displays the (S, G) multicast forwarding entries.

For command in step 4, when this command does not contain any option, all the multicast route entries are deleted.

Example This example shows how to view IP multicast routing table.

```
ZXR10#show ip mroute
IP Multicast Routing Table
Flags:D -Dense,S -Sparse,C -Connected,L -Local,P -Pruned
      R -RP-bit set,F -Register flag,T -SPT-bit set,J -Join SPT,
      M - MSDP created entry,N -No Used,U -Up Send,
      A - Advertised via MSDP,X -Proxy Join Timer Running,
      * -Assert flag
Statistic: Receive packet count/Send packet count
Timers:Uptime/Expires
Interface state:Interface,Next-Hop or VCD,State/Mode

(*, 229.3.3.16), 00:00:01/00:03:34, RP 5.5.5.6 , 0/0, flags: SP
  Incoming interface: vlan5, RPF nbr 5.5.5.6
  Outgoing interface list: NULL
(100.1.1.100, 229.3.3.16), 00:00:01/00:03:34 , 0/0, flags: UN
  Incoming interface: vlan4, RPF nbr 4.4.4.5
  Outgoing interface list:
    Vlan6, Forward/Sparse, 00:00:01/00:03:29
```

This example shows how to view multicast forwarding route entries.

```
ZXR10#show ip forwarding mroute module 7
group-address 229.3.3.16

IP Forwarding Multicast Routing Table
Flags: N -No Used,U -Up Send,L -Limit upSend,A - Assert send

(*, 229.3.3.16), Flags:, HitFlag:0, Incoming interface: Null,
LastSrcIp: 0.0.0.0
  Outgoing vlan interface list: NULL

L2bitmap:0x0000000000000000 L3bitmap:0x0000000000000000

(100.1.1.100, 229.3.3.16), Flags:, HitFlag:0, Incoming interface:
vlan4 19/3, LastSrcIp: 0.0.0.0
  Outgoing vlan interface list: NULL

L2bitmap:0x4000000000000008 L3bitmap:0x0000000000000000
```

IGMP Maintenance and Diagnosis

To configure IGMP maintenance and diagnosis, perform the following steps.

Step	Command	Function
1	<code>ZXR10#show ip igmp interface [<interface-name>]</code>	This displays IGMP configuration information on interface
2	<code>ZXR10#show ip igmp groups [<interface-name>]</code>	This displays IGMP group joining information on an interface

**Note:**

IGMP configuration information includes current IGMP version, query router ID, query time interval and max response time.

Example This example shows how to view IGMP configuration information on interface vlan4.

```
ZXR10#show ip igmp interface vlan4
vlan4
  Internet address is 4.4.4.4, subnet mask is 255.255.255.0
  IGMP is enabled on interface
  Current IGMP version is 2
  IGMP query interval is 125 seconds
  IGMP last member query interval is 1 seconds
  IGMP query max response time is 10 seconds
  IGMP querier timeout period is 251 seconds
  IGMP querier is 4.4.4.4, never expire
  Inbound IGMP access group is not set
  IGMP immediate leave control is not set
```

This example shows how to view the group member information on interface vlan1.

```
ZXR10#show ip igmp groups vlan 1
IGMP Connected Group Membership
Group addr   Interface   Present    Expire     Last Reporter
224.1.1.1    vlan1       00:00:48   never       4.4.4.4
```

PIM-SM Maintenance and Diagnosis

To configure PIM-SM maintenance and diagnosis, perform the following steps.

Step	Command	Function
1	<code>ZXR10#show ip pim bsr</code>	This displays BSR information
2	<code>ZXR10#show ip pim rp mapping</code>	This displays information of RP set that is advertised by BSR
3	<code>ZXR10#show ip pim rp hash <group-address></code>	This displays information of RP that is selected by a specific multicast group
4	<code>ZXR10#show ip pimsm interface [<interface-name>]</code>	This displays information of PIM-SM interface
5	<code>ZXR10#show ip pimsm neighbor [<interface-name>]</code>	This displays peer information of PIM-SM interface

Example This example shows the BSR information.

```
ZXR10#show ip pim bsr
Uptime: 00:00:11, BSR Priority :0, Hash mask length:30
Expires:00:00:49
This system is a candidate BSR
  candidate BSR address: 6.6.6.6,priority: 0,hash mask length: 30
This System is Candidate_RP:
  candidate RP address: 6.6.6.6(vlan6),priority:192
```

This example shows how to view information of RP set that is advertised by BSR.

```
ZXR10#show ip pim rp mapping
Group(s) 224.0.0.0/4
  RP 5.5.5.6 static, Priority :192
  RP 6.6.6.6 <?>, :v2, Priority :192
  BSR: 6.6.6.6 <?>, via bootstrap
Uptime: 00:00:14, expires: 00:02:16
```

This example shows how to view information of RP that is selected by group 224.1.1.1.

```
ZXR10#show ip pim rp ha 224.1.1.1
rp address:5.5.5.6 static
```

This example shows how to view information of PIM-SM interface.

```
ZXR10#show ip pimsm interface
Address Interface State Nbr Query DRCountIntvl DRPriority
4.4.4.4 vlan4 Up 0 30 4.4.4.4 1
5.5.5.5 vlan5 Up 0 30 5.5.5.5 1
6.6.6.6 vlan6 Up 0 30 6.6.6.6 1
0.0.0.0 vlan100 Down 0 30 0.0.0.0 1
```

This example shows how to view peer information of PIM-SM interface.

```
ZXR10#show ip pimsm neighbor
Neighbor Address Interface DR Prio Uptime Expires
131.1.1.91 vlan4 30000 00:19:34 00:01:29
22.22.22.43 vlan5 1 03:21:25 00:01:16
```

MSDP Maintenance and Diagnosis

To configure MSDP maintenance and diagnosis, perform the following steps.

Step	Command	Function
1	ZXR10# show ip msdp count	This displays number of SA messages from each MSDP peer in SA cache
2	ZXR10# show ip msdp peer [<peer-address>]	This displays detailed information of MSDP peers
3	ZXR10# show ip msdp sa-cache [<group-address>[<source-address>]]	This displays (S, G) states of each MSDP peer
4	ZXR10# show ip msdp summary	This displays MSDP peer state

Example This example shows how to view statistics information of SA messages.

```
ZXR10#show ip msdp count
SA State per Peer Counters, <Peer>: <# SA learned>
101.1.1.1: 2
```

```

102.2.2.2: 20
103.3.3.3: 10

Total entries: 32

```

This example shows how to view detailed information of MSDP peers.

```

ZXR10#show ip msdp peer
MSDP Peer 11.1.1.1
Description:
  Connection status:
    State: Down, Resets: 0, Connection source: vlan4 (4.4.4.4)
    Uptime(Downtime): 00:00:04, Messages sent/received: 0/0
    Connection and counters cleared 00:00:04 ago
  SA Filtering:
    Input (S,G) filter: none
    Output (S,G) filter: none
  Peer ttl threshold: 0
  SAs learned from this peer: 0

```

This example shows how to view (S, G) states of each MSDP peer.

```

ZXR10#show ip msdp sa-cache
MSDP Source-Active Cache - 4 entries
(101.101.101.101, 224.1.1.1), RP 49.4.4.4, 00:21:45/ 00:05:57
(101.101.101.101, 224.1.1.2), RP 49.4.4.4, 00:21:45/ 00:05:57
(101.101.101.101, 226.1.1.1), RP 50.4.4.4, 00:09:04/ 00:04:57
(101.101.101.101, 226.1.1.2), RP 50.4.4.4, 00:09:04/ 00:04:57

```

This example shows how to view MSDP peer state.

```

ZXR10#show ip msdp summary
MSDP Peer Status Summary
Peer Address State Uptime/Downtime ResetCount SACount
101.1.1.1 Up 1d10h 9 2
*102.2.2.2 Up 14:24:00 5 20
103.3.3.3 Up 12:36:17 5 10

```

Static IP Multicast Maintenance and Diagnosis

To configure static IP multicast maintenance and diagnosis, perform the following steps.

Step	Command	Function
1	ZXR10#show ip multicast-static-interface [index <1-100>]	This shows index interface set
2	ZXR10#show ip multicast-static-route [group <address> source <address> summary]	This shows static IP multicast route entries

Policy Routing Backup Configuration

Table of Contents

Overview	95
Configuring Policy Routing Backup	95
Policy Routing Backup Maintenance and Diagnosis.....	96

Overview

Function Introduction	To implement policy routing function on switch, execute Redirect command based on ACL. As for each ACL rule, route can be redirected to only one next-hop. When this next hop is down, corresponding policy routing will get invalid. When there are multiple outgoing interfaces on the switch, redirect route to multiple next-hops by configuring Redirect. When the master link is down, it switches to the backup next hop automatically. Then policy routing backup (PBR BACK) function is implemented.
Principle	Specify priority for each next hop when configuring redirect to multiple next hops. When the currently used next hop with high priority is down, it will switch to the next hop with sub-high priority with the switchover time within one second. It is available to configure whether to switch back to the next hop with high priority restores after it restores normal.

Configuring Policy Routing Backup

Short Description	To implement policy routing backup function, configure redirect function, which can specify multiple next hops.
--------------------------	---

Command	Function
<pre> ZXR10(config)#redirect in {<acl-no> <acl-name>} rule-id <rule-no>{cpu interface <port-name> {[next-hop1 <ip-addr><0-7>],[next-hop2 <ip-addr><0-7</pre>	This configures redirect function in global configuration mode and the number of configured next hops is 8 at most.

Use command **no redirect** {<acl-no>|<acl-name>} **rule-id** <rule-no> to delete redirect configuration.

Parameters:

Parameter	Description
acl-no acl-name	ACL number ACL name, acl-no ranges from 1 to 349 and from 1000 to 3499.
rule-id	This is the number of ACL rule, ranging from 1 to 1000
cpu	This redirects to CPU.
interface	This redirects to the designated interface.
next-hop	This specifies IP address of the next hop (used for policy routing).
next-hop1	This specifies IP address of the next hop (used for policy routing).
next-hop2	This specifies IP address of the next hop (used for policy routing).
next-hop3	This specifies IP address of the next hop (used for policy routing).
next-hop4	This specifies IP address of the next hop (used for policy routing).
next-hop5	This specifies IP address of the next hop (used for policy routing).
next-hop6	This specifies IP address of the next hop (used for policy routing).
next-hop7	This specifies IP address of the next hop (used for policy routing).
next-hop8	This specifies IP address of the next hop (used for policy routing).

Policy Routing Backup Maintenance and Diagnosis

Short Description By executing command **show**, related information of specific ACL and configuration entries related to PBR BACK can be viewed.

Command	Function
<pre> ZXR10(config)#show qos [{number <acl-number> name <acl-name>}][rule-id <rule-no>]]</pre>	This shows QoS configuration information.

Parameters:

Parameter	Description
acl-number	This is ACL number, ranging from 1 to 349 and from 1000 to 3499.
acl-name	This is ACL name.
rule-id	This is the number of ACL rule, ranging from 1 to 1000

This page is intentionally blank.

IP/LDP FRR Configuration

Table of Contents

IP/LDP FRR Overview	99
Configuring IP/LDP FRR	101
IP/LDP FRR Configuration Example.....	103
IP/LDP FRR Maintenance and Diagnosis	106

IP/LDP FRR Overview

When the link or node is unavailable in network, the packet that flows through these unavailable nodes will be discarded or become loopback. As a result, the temporary traffic interruption or loopback will be inevitable to occur until the new topology and route is recalculated. The interruption period usually lasts several seconds. Currently, some novel technologies compress the convergence time to below 1 second. However, with the network size has become larger and larger, and all kinds of new applications emerge in endlessly, especially some applications are very sensitive for traffic interruption, such as voice and media, the fast recovery of traffic becomes particularly important.

Node Fault Recovery Analysis

The network convergence period has three levels now, as shown below.

- Sub-Second (second level)
Most of IP networks have such requirement, and the current technology can satisfy it.
- Sub-500ms (500 milliseconds)
This objective can be reached and it is being captured.
- Sub-50ms (50 milliseconds)
This is a business requirement for some specified parts in IP network. It can not be reached now.

The convergence time usually are cost in the following aspects.

1. The Time is to discovery unavailable node and link. The examine time is 10-odd milliseconds for unavailable physical link. The examine time is tens seconds for unavailable hello hold-time in protocol layer.

2. The time is to notice the unavailable event to router's controller layer. It costs several milliseconds to 10-odd milliseconds.
3. The time is to take the corresponding responses to the unavailable node and link. The response implies that trigger and floods the new link state updating packet, usually is several milliseconds to 10-odd milliseconds.
4. The time is to notice the other nodes in network that the local router link is unavailable. Each node costs several milliseconds to a hundred seconds usually.
5. The time is to recalculate the trigger route. For IGP protocol using Dijkstra arithmetic, the time is 10-odd milliseconds.
6. The time is to calculate the new routing information with line card, and form the forwarding table. The cost time varies from the different routing entries number, usually is several hundred milliseconds.
7. The time is to record the new forwarding route entries into hardware. It costs 10-odd milliseconds.

The traffic losing is occurred in the above mentioned steps, it can be divided into two stages as follows.

1. Stage 1: The router can not discovery the unavailable link immediately, and it still forwards the traffic to the unavailable link.
2. Stage 2: The route has found the unavailable link, but the network is in convergence process. The local forwarding table is different with other router's, which causes "micro-loop" in forwarding layer.

IP FRR Functions

To decrease the traffic interruption period, a mechanism has to be provided to realize the following requirements.

- Fast discovery of unavailable link.
- When the link is unavailable, fast provide a recovery path.
- Prevent forwarding loopback "micro-loop" occurs during the further recovery process.

IP Fast Rerouter (IP FRR) technology is adopted to satisfy the above requirements.

IP FRR Working Procedure

The working procedure of IP FRR is shown below.

1. Examine the failure fast. The common technologies include BFD and physical signal examine.
2. Modify the forwarding plane. Switch the traffic into the recalculated backup path.
3. Perform route re-convergence.
4. After finishing the re-convergence, switch the route to the optimal path.

Obviously, the backup path is to fill the FRR gap up, which switches the traffic to the backup next hop, to guarantee the traffic will not be interrupted.

LDP FRR Overview

In MPLS area, the link or node failure causes the unavailable LSP and the interrupt MPLS traffic. Similar with IP FRR, LDP FRR is a mechanism to guarantee the traffic can be fast recovered in MPLS area. Redirect MPLS traffic to the backup path that is specified by IGP is doable, because MPLS traffic path is specified by IGP.

The working flow of LDP FRR is shown below.

1. The route protocol advertises the optimal and IP FRR backup path to LDP, LDP records their corresponding labels into for-

- warding layer. Before the failure occurs, MPLS traffic is forwarded according to the optimal path.
2. The forwarding layer switches MPLS traffic to IP FRR backup path for forwarding after the failure is examined.
 3. After finishing the route re-convergence, forwarding layer switches MPLS traffic to the optimal path.

Configuring IP/LDP FRR

Configuring OSPF FRR

To configure OSPF FRR, perform the following steps.

1. To enter OSPF configuration mode, use the following command.

Command	Function
ZXR10 (config) # router ospf <ospfid>	This enters OSPF configuration mode

2. To enable FRR function and choose calculation policy of backup route, use the following command.

Command	Function
ZXR10 (config-router) # fast-reroute alternate-protect-type { default down-stream-path }	This enables FRR function and chooses calculation policy of backup route

3. To enter interface configuration mode, use the following command.

Command	Function
ZXR10 (config) # interface vlan <vlanid >	This enters interface configuration mode

4. To configure a backup interface, use the following command.

Command	Function
ZXR10 (config-if) # ip ospf fast-reroute backup-interface <interface-name>	This configures a backup interface

To cancel a backup interface, use **no ip ospf fast-reroute** command.

Configuring IS-IS FRR

To configure IS-IS FRR, perform the following steps.

1. To enter IS-IS configuration mode, use the following command.

Command	Function
ZXR10(config)# router isis	This enters IS-IS configuration mode

2. To enable FRR function, use the following command.

Command	Function
ZXR10(config-router)# fast-reroute enable	This enables FRR function and use default calculation policy of backup route, that is, LFAs

3. To change FRR calculation mode, use the following command.

Command	Function
ZXR10(config-router)# fast-reroute alternate-type down-stream-path	This changes FRR calculation mode

4. To enter interface configuration mode, use the following command.

Command	Function
ZXR10(config)# interface vlan <vlanid>	This enters interface configuration mode

5. To block an interface to participate in calculation of backup route, use the following command.

Command	Function
ZXR10(config-if)# isis fast-reroute block	This blocks an interface to participate in calculation of backup route

Configuring BGP FRR

To configure BGP FRR, perform the following steps.

Step	Command	Function
1	ZXR10 (config) # router bgp <1-65535>	This enters BGP configuration mode
2	ZXR10 (config-router) # bgp frr	This enables BGP FRR

Configuring LDP FRR

LDP FRR is based on IGP FRR. Enable LDP protocol on the basis of IGP FRR configuration, which forms LDP FRR configuration.

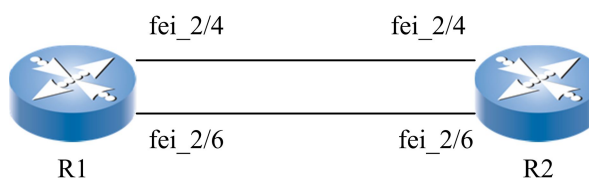
IP/LDP FRR Configuration Example

OSPF FRR Configuration Example

This example describes how to configure OSPF FRR.

As shown in [Figure 28](#), R1 and R2 run OSPF protocol, and FRR function is enabled on R1.

FIGURE 28 OSPF FRR CONFIGURATION EXAMPLE



R1 configuration:

```

ZXR10_R1(config)#interface fei_2/4
ZXR10_R1(config-if)#ip address 192.168.15.1 255.255.255.0
ZXR10_R1(config-if)#ip ospf cost 1
ZXR10_R1(config-if)#exit
ZXR10_R1(config)#interface fei_2/6
ZXR10_R1(config-if)#ip address 192.168.100.1 255.255.255.0
ZXR10_R1(config-if)#ip ospf cost 2
ZXR10_R1(config-if)#exit
ZXR10_R1(config)#router ospf 1
ZXR10_R1(config-router)#network 192.168.15.1 0.0.0.0 area 0
ZXR10_R1(config-router)#network 192.168.100.1 0.0.0.0 area 0
ZXR10_R1(config-router)#fast-reroute
alternate-protect-type default
  
```

R2 configuration:

```

ZXR10_R2(config)#interface fei_2/4
ZXR10_R2(config-if)#ip address 192.168.15.2 255.255.255.0
ZXR10_R2(config-if)#exit
ZXR10_R2(config)#interface fei_2/6
ZXR10_R2(config-if)#ip address 192.168.100.2 255.255.255.0
  
```

```

ZXR10_R2(config-if)#exit
ZXR10_R2(config)#router ospf 2
ZXR10_R2(config-router)#network 192.168.15.2 0.0.0.0 area 0
ZXR10_R2(config-router)#network 192.168.100.2 0.0.0.0 area 0
ZXR10_R2(config-router)#exit

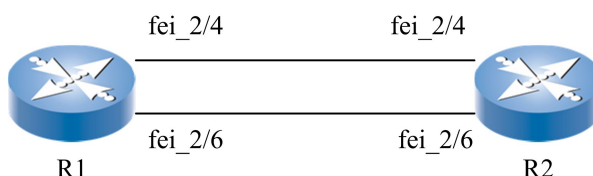
```

IS-IS FRR Configuration Example

This example describes how to configure IS-IS FRR.

As shown in [Figure 29](#), R1 and R2 run IS-IS protocol, FRR function is enabled on R1.

FIGURE 29 IS-IS FRR CONFIGURATION EXAMPLE



R1 configuration:

```

ZXR10_R1(config)#router isis
ZXR10_R1(config-router)#area 01
ZXR10_R1(config-router)#system-id 00D0.D0C7.53E0
ZXR10_R1(config-router)#exit
ZXR10_R1(config)#interface fei_2/4
ZXR10_R1(config-if)#ip address 192.168.15.1 255.255.255.0
ZXR10_R1(config-if)#ip router isis
ZXR10_R1(config-if)#isis metric 5
ZXR10_R1(config-if)#exit
ZXR10_R1(config)#interface fei_2/6
ZXR10_R1(config-if)#ip address 192.168.100.1 255.255.255.0
ZXR10_R1(config-if)#ip router isis
ZXR10_R1(config-if)#exit
ZXR10_R1(config)#router isis
ZXR10_R1(config-router)#fast-reroute enable
ZXR10_R1(config-router)#exit

```

R2 configuration:

```

ZXR10_R2(config)#router isis
ZXR10_R2(config-router)#area 00
ZXR10_R2(config-router)#system-id 00D0.E0D7.53E0
ZXR10_R2(config-router)#exit
ZXR10_R2(config)#interface fei_2/4
ZXR10_R2(config-if)#ip address 192.168.15.2 255.255.255.0
ZXR10_R2(config-if)#ip router isis
ZXR10_R2(config-if)#exit
ZXR10_R2(config)#interface fei_2/6
ZXR10_R2(config-if)#ip address 192.168.100.2 255.255.255.0
ZXR10_R2(config-if)#ip router isis
ZXR10_R2(config-if)#exit

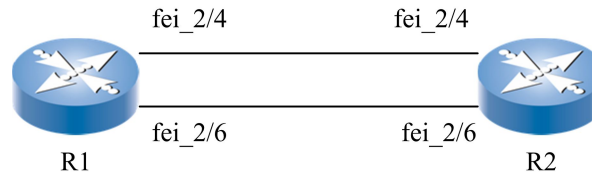
```

BGP FRR Configuration Example

This example describes how to configure BGP FRR.

As show in [Figure 30](#), R1 and R2 run BGP protocol, FRR function is enabled on R1. R2 redistributes static routes, and the master/slave routes are formed on R1.

FIGURE 30 BGP FRR CONFIGURATION EXAMPLE



R1 configuration:

```
ZXR10_R1(config)#interface fei_2/4
ZXR10_R1(config-if)#ip address 192.168.15.1 255.255.255.0
ZXR10_R1(config-if)#exit
ZXR10_R1(config)#interface fei_2/6
ZXR10_R1(config-if)#ip address 192.168.100.1 255.255.255.0
ZXR10_R1(config-if)#exit
ZXR10_R1(config)#router bgp 100
ZXR10_R1(config-router)#neighbor 192.168.15.2 remote-as 200
ZXR10_R1(config-router)#neighbor 192.168.100.2 remote-as 200
ZXR10_R1(config-router)#bgp frr
ZXR10_R1(config-router)#exit
```

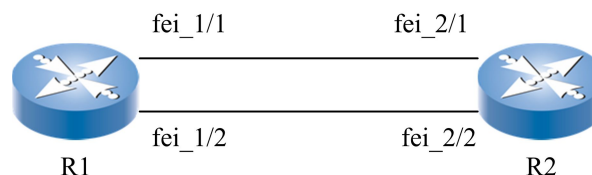
R2 configuration:

```
ZXR10_R2(config)#interface fei_2/4
ZXR10_R2(config-if)#ip address 192.168.15.2 255.255.255.0
ZXR10_R2(config-if)#exit
ZXR10_R2(config)#interface fei_2/6
ZXR10_R2(config-if)#ip address 192.168.100.2 255.255.255.0
ZXR10_R2(config-if)#exit
ZXR10_R2(config)#router bgp 200
ZXR10_R2(config-router)#neighbor 192.168.15.1 remote-as 100
ZXR10_R2(config-router)#neighbor 192.168.100.1 remote-as 100
ZXR10_R2(config-router)#redistribute static
ZXR10_R2(config-router)#exit
```

LDP FRR Configuration Example

This example describes how to configure LDP FRR based on OSPF FRR. Network topology is shown in [Figure 31](#).

FIGURE 31 LDP FRR CONFIGURATION EXAMPLE



R1 configuration:

```
ZXR10_R1(config)#mpls ip
ZXR10_R1(config)#interface Loopback1
ZXR10_R1(config-if)#ip address 10.10.1.1 255.255.255.255
ZXR10_R1(config-if)#exit
ZXR10_R1(config)#interface fei_1/1
ZXR10_R1(config-if)#ip address 10.10.12.1 255.255.255.0
ZXR10_R1(config-if)#mpls ip
```

```

ZXR10_R1(config)#interface fei_1/2
ZXR10_R1(config-if)#ip address 10.10.23.1 255.255.255.0
ZXR10_R1(config-if)#mpls ip
ZXR10_R1(config-if)#ip ospf cost 20
ZXR10_R1(config-if)#exit
ZXR10_R1(config)#router ospf 1
ZXR10_R1(config-router)#network 10.0.0.0 0.255.255.255 area 0
ZXR10_R1(config-router)#fast-reroute
alternate-protect-type default

```

R2 configuration:

```

ZXR10_R2(config)#mpls ip
ZXR10_R2(config)#interface Loopback1
ZXR10_R2(config-if)#ip address 10.10.2.2 255.255.255.255
ZXR10_R2(config-if)#exit
ZXR10_R2(config)#interface fei_2/1
ZXR10_R2(config-if)#ip address 10.10.12.2 255.255.255.0
ZXR10_R2(config-if)#mpls ip
ZXR10_R2(config)#interface fei_2/2
ZXR10_R2(config-if)#ip address 10.10.23.2 255.255.255.0
ZXR10_R2(config-if)#mpls ip
ZXR10_R2(config-if)#exit
ZXR10_R2(config)#mpls ldp router-id loopback1
ZXR10_R2(config)#router ospf 1
ZXR10_R2(config-router)#network 10.0.0.0 0.255.255.255 area 0

```

IP/LDP FRR Maintenance and Diagnosis

To configure LDP FRR maintenance and diagnosis, perform the following steps.

Step	Command	Function
1	ZXR10#show isis fast-reroute-topology [level-1 level-2]	This displays the backup topology relationship
2	ZXR10#show ip backup route	This displays the backup route
3	ZXR10#show ip ospf border-lfas [process <process-id>]	This displays the backup routes of master router
4	ZXR10#debug ip ospf fast-reroute [intra][inter][external][nbrspf]	This displays the calculation of backup route

BFD Configuration

Table of Contents

BFD Overview	107
Configuring BFD	108
BFD Configuration Example	109
BFD Maintenance and Diagnosis	110

BFD Overview

Network device requires the communication failure between the adjacency systems can be fast examined. Thus, the substitute path can be fast created, or the traffic can be switched to other link when the failure occurs.

The presentation of Bidirectional Forwarding Detection (BFD) provides a solution for the above requirement. BFD can examine failure at any channel between systems. These channels include the direct connected physical link, virtual link and tunnel, MPLS LSP, and multi-hop route channel, non-direct connected channel. Meanwhile, BFD is concentrated on how to fast examine the forwarding failure because of its singleness and simplicity, which helps the network to realize voice, media and other on demand services by excellent QoS. As a result, service provider can provide high reliability and applicability VoIP and other real-time services based on IP network for users.

BFD is a low load method, which fast examine the failure occurs between the two adjacent forwarding engines. The failure can exist in interface or data link, and even exist in the forwarding engine itself. BFD also provides a single examine mechanism for various mediums, such as any protocol layer. BFD examines the failure by communicating with forwarding engine of the next-hop. The forwarding engine is separated with control engine. That means the protocol is bound with forwarding layer, and the protocol is separated from routing protocol engine (the control layer).

BFD can be considered as a simple "Hello" protocol. Two routers send BFD packet on each path periodically. It is confirmed that the bidirectional path from system to neighbor is failure if the system fails to receive packet in a period of time. For some special cases, router can negotiate to stop sending BFD packet periodically, which decreases the load.

Configuring BFD

To configure BFD, perform the following steps.

1. To configure basic BFD parameters, use the following command.

Command	Function
ZXR10(config-if) # bfd interval <milliseconds> min_rx <milliseconds> multiplier <multiplier-value>	This configures basic BFD parameters

Parameter descriptions:

Parameter	Description
interval <milliseconds>	Specify the minimal time interval for sending BFD packet
min_rx <milliseconds>	Specify the minimal time interval for receiving BFD packet
multiplier <multiplier-value>	Specify the examine multiplier of BFD packet

2. To enable BFD function in different modules, use one of the following commands.

Command	Function
ZXR10(config-router) # ip ospf bfd	This enables BFD in OSPF
ZXR10(config-router) # isis bfd	This enables BFD in IS-IS
ZXR10(config-router) # neighbor <ip-address> fall-over bfd	This enables BFD in BGP

3. To clear designated BFD session, use the following command.

Command	Function
ZXR10# clear bfd session <address session-address> <discriminator discr-number>	This clears designated BFD session

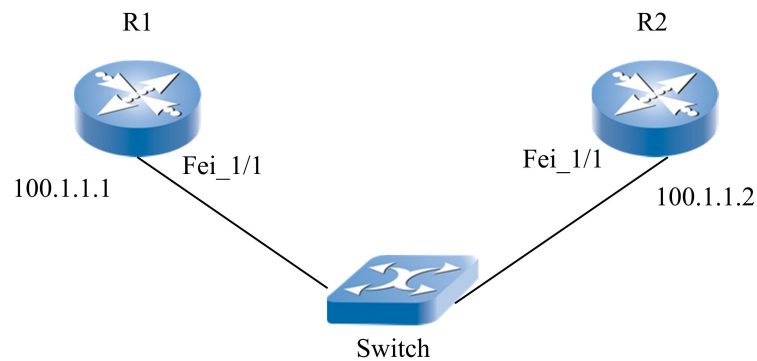
4. To configure RSVP BFD, use the following command.

Command	Function
ZXR10(config-if) # ip rsvp bfd	This configures RSVP BFD

BFD Configuration Example

This example shows how to create a connection by binding BFD to RSVP-TE LSP, and create a connection by configuring BFD on the base of MPLS label. Network topology is shown in [Figure 32](#).

FIGURE 32 BFD CONFIGURATION EXAMPLE



R1 configuration:

```

R1(config)#mpls traffic-eng tunnels

R1(config)#interface fei_1/1
R1(config-if)#ip address 100.1.1.1 255.255.255.0

R1(config)#interface loopback1
R1(config-if)#ip address 100.0.0.1 255.255.255.255

R1(config)#router ospf 1
R1(config-router)#network 0.0.0.0 255.255.255.255 area 1
R1(config-router)#mpls traffic router-id loopback1
R1(config-router)#mpls traffic area 1

R1(config)#interface tunnel1
R1(config-if)#tunnel mode mpls traffic-eng
R1(config-if)#tunnel destination ipv4 100.0.0.2
R1(config-if)#tunnel mpls traffic-eng path-option 1
explicit-path identifier 1
R1(config)#ip explicit-path identifier 1
next-address 100.1.1.2 strict

R1(config)#interface tunnel1
R1(config-if)#tunnel mpls traffic-eng bfd

R1(config)#show bfd neighbors rsvp-lsp
Tunnel      LD      RD      Hold   State   Int
tunnel1      2        2      150    UP      fei_1/1
R2(config) #sho bfd neighbors rsvp-lsp
OurAddr  NeighAddr  LD  RD  Holddown  mult  State  Int
100.1.1.1 100.1.1.2  2   2   150       3    UP    fei_1/1

R1(config)#show bfd neighbor detail
Registered protocols: RSVP LSP
  
```

R2 configuration:

```

R2(config)#mpls traffic-eng tunnels

R2(config)#interface fei_1/1
R2(config-if)#ip address 100.1.1.2 255.255.255.0

R2(config)#interface loopback1
R2(config-if)#ip address 100.0.0.2 255.255.255.255

R2(config)#router ospf 1
  
```

```
R2(config-router)#network 0.0.0.0 255.255.255.255 area 1
R2(config-router)#mpls traffic router-id loopback1
R2(config-router)#mpls traffic area 1
```

BFD Maintenance and Diagnosis

To configure BFD maintenance and diagnosis, perform the following steps.

1. To display BFD session information, use the following command.

Command	Function
ZXR10# show bfd neighbors {brief detail}	This displays BFD session information

This example shows brief BFD session information.

```
ZXR10#show bfd neighbors
OurAddr      NeighAddr    LD/RD RH Holdown(mult) State  Int
172.16.10.1  172.16.10.2  1/6   1   260 (3 )    Up    Fa0/1
```

This example shows detailed BFD session information.

```
OurAddr      NeighAddr    LD/RD RH Holdown(mult) State  Int
172.16.10.1  172.16.10.2  1/2   1   460 (3 )    Up    Fa0/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 1000, Received Multiplier: 3
Holdown (hits): 600(0), Hello (hits): 200(390169)
Rx Count: 229225, Rx Interval (ms) min/max/avg:
208/440/332 last: 144 ms ago
Tx Count: 388219, Tx Interval (ms) min/max/avg:
148/248/196 last: 48 ms ago
Registered protocols: OSPF Stub
Uptime: 17:44:37
Last packet: Version: 0 - Diagnostic: 0
I Hear You bit: 1 - Demand bit: 0
Poll bit: 0 - Final bit: 0
```

2. To debug BFD, use the following command.

Command	Function
ZXR10# debug bfd [event packet error]	This debugs BFD

This example shows BFD event debugging information.

```
ZXR10#debug bfd event
22:56:35: BFD: bfd neighbor - action:CREATE, proc:1024,
idb:FastEthernet0/1, neighbor:172.16.10.2
22:56:37: Session [172.16.10.1,172.16.10.2,Fa0/1,1],
event RX IHY 0, state FAILING -> DOWN
22:56:37: Session [172.16.10.1,172.16.10.2,Fa0/1,1],
event RX IHY 0, state DOWN -> INIT
22:56:37: Session [172.16.10.1,172.16.10.2,Fa0/1,1],
event RX IHY 1, state INIT -> UP
```

Figures

Figure 1 Static Route Configuration	4
Figure 2 Static Route Aggregation Configuration Example	5
Figure 3 Default Route Configuration Example	6
Figure 4 RIP Configuration Example	14
Figure 5 OSPF Router Types	21
Figure 6 Basic OSPF Configuration Example.....	29
Figure 7 Multi-Area OSPF Configuration Example.....	30
Figure 8 OSPF Virtual Link Configuration Example	32
Figure 9 OSPF Authentication Configuration Example.....	33
Figure 10 IS-IS Area	36
Figure 11 Single-Area IS-IS Configuration Example.....	41
Figure 12 Multi-Area IS-IS Configuration Example.....	42
Figure 13 Basic BGP Configuration	47
Figure 14 BGP Route Advertisement Configuration	48
Figure 15 BGP Route Aggregation Configuration.....	49
Figure 16 EBGP Multi-Hop Configuration	50
Figure 17 Filtering Routes through NLRI	52
Figure 18 Filtering Routes through AS_PATH Attribute	53
Figure 19 LOCAL_PREF Attribute Configuration	54
Figure 20 MED Attribute Configuration.....	55
Figure 21 Configuring BGP Synchronization	58
Figure 22 BGP Route Reflector.....	60
Figure 23 BGP Confederation.....	61
Figure 24 BGP Configuration Example.....	63
Figure 25 Load Sharing Configuration Example	66
Figure 26 Static IP Multicast Configuration Example	79
Figure 27 IP Multicast Configuration Example	89
Figure 28 OSPF FRR Configuration Example.....	103
Figure 29 IS-IS FRR Configuration Example.....	104
Figure 30 BGP FRR Configuration Example	105
Figure 31 LDP FRR Configuration Example.....	105
Figure 32 BFD Configuration Example.....	109

This page is intentionally blank.

Tables

Table 1 CHAPTER SUMMARY i

Table 3 OSPF Authentication 23

This page is intentionally blank.

List of Glossary

ABR - Area Border Router
AD - Administrative Distance
AS - Autonomous System
ASBR - Autonomous System Border Router
BDR - Backup Designate Router
BGP - Border Gateway Protocol
BSR - Bootstrap Router
CIDR - Classless Inter-Domain Routing
CLNS - ConnectionLess Network Service
DIS - Designate IS
DR - Designate Router
EBGP - External Border Gateway Protocol
FRR - Fast Reroute
IBGP - Interior Border Gateway Protocol
IGMP - Internet Group Management Protocol
IGP - Interior Gateway Protocol
IS-IS - Intermediate System-to-Intermediate System
ISO - International Organization for Standardization
ISP - Internet Service Provider
LDP - Label Distribution Protocol
LSA - Link State Advertisement
LSU - Link State Update
MD5 - Message Digest 5
MED - MULTI_EXIT_DISC
MPLS - Multi-Protocol Label Switching
MSDP - Multicast Source Discovery Protocol
NBMA - Non-Broadcast Multiple Access
NLRI - Network Layer Reachable Information
NSSA - Not-So-Stubby Area
OSI - Open Systems Interconnection
OSPF - Open Shortest Path First
PDU - Protocol Data Unit
PIM-SM - Protocol Independent Multicast Sparse Mode
RFC - Request For Comments
RIP - Routing Information Protocol

RP - Rendezvous Point

RPF - Reverse Path Forwarding

RR - Router Reflector

SNP - Sequence Num PDU

SPF - Shortest Path First

TCP - Transmission Control Protocol

UDP - User Datagram Protocol

VLSM - Variable Length Subnet Mask